Question #1 *Topic 1*

You are configuring project metrics for dashboards in Azure DevOps.
You need to configure a chart widget that measures the elapsed time to complete work items once they become active.
Which of the following is the widget you should use?

A. Cumulative Flow Diagram

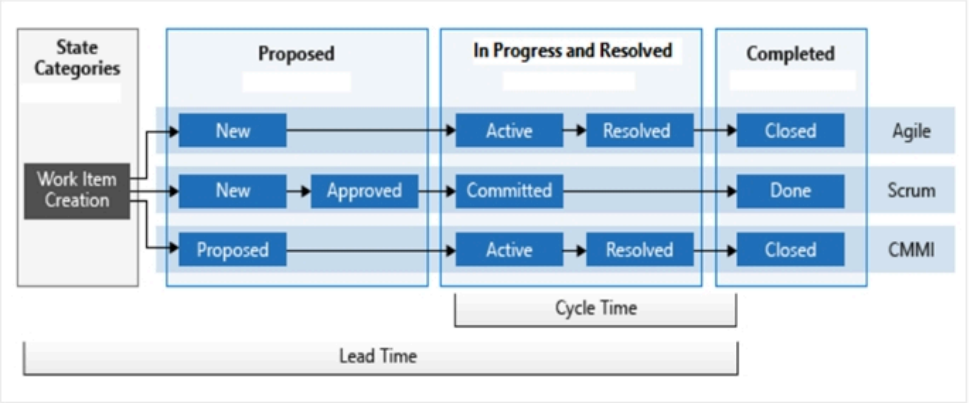
B. Burnup

C. Cycle time

D. Burndown

Suggested Answer: *C*
Cycle time measures the time it takes for your team to complete work items once they begin actively working on them.
Reference:
https://docs.microsoft.com/en-us/azure/devops/report/dashboards/cycle-time-and-lead-time?view=vsts

The following diagram illustrates how lead time differs from cycle time. Lead time is calculated from work item creation to entering a completed state. Cycle time is calculated from first entering an In Progress or Resolved state category to entering a Completed state category. To understand how workflow states map to state categories, see How workflow states and state categories are used in Backlogs and Boards.



Community vote distribution
C (100%)

Realdumpscollection_com_web Highly Voted 2 months ago
Selected Answer: C
Cycle time - This is used to look at the time taken to close a work item after work on it has started. C is right answer
upvoted 12 times

Cubbywoo Highly Voted 1 year, 7 months ago
C. Cycle time

A. Cumulative Flow Diagram shows the number of work items in different states over time and can be used to monitor progress and identify bottlenecks, but it doesn't specifically measure elapsed time.

B. Burnup charts show the progress of completed work items over time and can be used to measure progress towards a goal, but it doesn't measure elapsed time once work items become active.

D. Burndown charts show the remaining work over time and can be used to measure progress towards completing a set of work items, but it doesn't measure elapsed time once work items become active.

Cycle time, on the other hand, specifically measures the elapsed time from when a work item becomes active to when it is completed, making it the best option to fulfill the requirement in the question.

#chatgpt
upvoted 11 times

karimullah Most Recent 3 weeks, 4 days ago
C is the rite answer
upvoted 1 times

dumps4azure_com 1 month ago
C is the rite answer.
upvoted 1 times

noobcloudsurfer 4 months, 2 weeks ago
Selected Answer: C
C. Cycle Time
Cycle time measures the time it takes for your team to complete work items once they begin actively working on them. It is calculated from first entering an In Progress or Resolved state category to entering a Completed state category.
Reference Diagram: -
https://learn.microsoft.com/en-us/azure/devops/report/dashboards/cycle-time-and-lead-time?view=azure-devops
If you need access to all 493 practice questions drop an email at dasdarpan269@gmail.com
upvoted 1 times

ChandraSingh 10 months, 2 weeks ago
C. Cycle time
upvoted 1 times

kleansoul 1 year ago
Selected Answer: C
Cycle time - This is used to look at the time taken to close a work item after work on it has started.
upvoted 1 times

Msds1981 1 year, 1 month ago
Selected Answer: C
C is correct
upvoted 1 times

zellck 1 year, 3 months ago
Selected Answer: C
C is the answer.

https://learn.microsoft.com/en-us/azure/devops/report/dashboards/cycle-time-and-lead-time?view=azure-devops
Both lead time and cycle time widgets are useful to teams. They both indicate how long it takes for work to flow through their development pipeline. Lead time measures the total time elapsed from the creation of work items to their completion. Cycle time measures the time it takes for your team to complete work items once they begin actively working on them.
upvoted 4 times

Rangnath 1 year, 5 months ago
Cycle Time
upvoted 2 times

sampath918 1 year, 5 months ago
Selected Answer: C
Cycle Time measures the time it takes to complete work items
upvoted 1 times

Realnaijaguy 1 year, 7 months ago
C-Cycle time/Keyword -ACTIVE
upvoted 2 times

[Removed] 1 year, 8 months ago
B pdf page 55
upvoted 1 times

DarioReymag 1 year, 9 months ago
B pdf page 55

upvoted 1 times

pandji 1 year, 10 months ago

It's C - Cycle time.

upvoted 3 times

nhannn 1 year, 10 months ago

Selected Answer: C

It's C - Cycle time.

upvoted 3 times

Hg6421 1 year, 10 months ago

Selected Answer: C

C for sure

upvoted 3 times

Question #2 *Topic 1*

You need to consider the underlined segment to establish whether it is accurate.
The Burnup widget measures the elapsed time from creation of work items to their completion.
Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required.

B. Lead time

C. Test results trend

D. Burndown

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/devops/report/dashboards/cycle-time-and-lead-time?view=vsts

Community vote distribution
B (100%)

megaejay Highly Voted 3 years, 2 months ago
correct Answer
upvoted 15 times

HV8282828282 Highly Voted 2 years, 6 months ago
Correct answer
This is really a strange way to word the question
upvoted 14 times

PrinceR Most Recent 11 months ago
Selected Answer: B
correct answer
upvoted 1 times

kleansoul 1 year ago
Selected Answer: B
Correct Answer

Lead time - This defines the time taken to close a work item after it has been created.
upvoted 2 times

sampath918 1 year, 5 months ago
Selected Answer: B
Lead time measures the total time elapsed from the creation of work items to their completion.
upvoted 1 times

sampath918 1 year, 5 months ago
GPT: The question is asking whether the underlined segment in the statement "The Burnup widget measures the elapsed time from creation of work items to their completion" is accurate or not.

The underlined segment in the statement is inaccurate because the Burnup widget does not measure the elapsed time from the creation of work items to their completion. Instead, the Burnup widget displays the progress of a project or iteration by tracking the total amount of work versus the completed work. It shows the total amount of work as a line chart, and the completed work as a bar chart, with the goal being to have the completed work reach the total amount of work by the end of the project or iteration.

Therefore, the accurate option to replace the underlined segment is "No, the Burnup widget does not measure the elapsed time from creation of work items to their completion." Option A, "No adjustment required," is not the correct answer in this case.
upvoted 1 times

Fal991l 1 year, 5 months ago

GPT:The underlined segment is inaccurate. The Burnup widget does not measure the elapsed time from creation of work items to their completion. Instead, it measures the progress towards completing a set of work items over time. Therefore, the accurate option is D, Burndown.
upvoted 1 times

Fal991l 1 year, 5 months ago
Bing:The selected text is asking you to consider whether the statement “The Burnup widget measures the elapsed time from creation of work items to their completion” is accurate. According to Microsoft’s documentation, burnup charts focus on completed work 1. Therefore, the statement is accurate, and option A) No adjustment required would be the correct answer
upvoted 1 times

Fal991l 1 year, 5 months ago
GPT:While it is true that burnup charts focus on completed work, the statement "The Burnup widget measures the elapsed time from creation of work items to their completion" is not accurate. Burnup charts measure progress towards completing a set of work items over time, not the elapsed time from creation to completion. Therefore, option A) No adjustment required is not the correct answer. The correct answer is option D) Burndown, which measures the progress of work remaining to complete a set of work items over time.
upvoted 1 times

Fal991l 1 year, 5 months ago
I am with GPT
upvoted 1 times

Cubbywoo 1 year, 7 months ago
The correct answer is "No adjustment required" because the underlined segment accurately describes what the Burnup widget measures.
upvoted 1 times

karrey 1 year, 4 months ago
Not true. The answer is lead time
upvoted 1 times

DarioReymag 1 year, 9 months ago
top command requires limit
upvoted 1 times

nhannn 1 year, 10 months ago
Selected Answer: B
It's B - Lead time.
upvoted 2 times

Hg6421 1 year, 10 months ago
Selected Answer: B
B correct
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: B
Answer is B for sure
upvoted 1 times

Govcomm 2 years, 1 month ago
Correct, B, lead time.
upvoted 1 times

kennynelcon 2 years, 2 months ago
Selected Answer: B
Lead Time

https://docs.microsoft.com/en-us/azure/devops/report/dashboards/cycle-time-and-lead-time?view=azure-devops
upvoted 3 times

rdemontis 2 years, 5 months ago
Selected Answer: B
correct
upvoted 2 times

AlMargoi 2 years, 9 months ago
B. - should be correct

upvoted 1 times

Question #3 *Topic 1*

You are making use of Azure DevOps manage build pipelines, and also deploy pipelines.
The development team is quite large, and is regularly added to.
You have been informed that the management of users and licenses must be automated when it can be.
Which of the following is a task that can't be automated?

A. Group membership changes

B. License assignment

C. Assigning entitlements

D. License procurement

Suggested Answer: *D*

Community vote distribution

D (84%) A (16%)

Eltooth Highly Voted 2 years, 4 months ago

Selected Answer: D

A, B and C can all be dynamic group membership.
D requires manual intervention.
upvoted 9 times

[Removed] Most Recent 4 months, 2 weeks ago

Selected Answer: D

Azure DevOps and Azure Active Directory offer automation for group memberships, license assignment, and assigning entitlements, license procurement typically requires manual intervention from an administrator to purchase licenses from a vendor.
upvoted 1 times

kleansoul 1 year ago

Selected Answer: D

License Procurement is a process which involves manual intervention. Rest all options can be dynamic.
upvoted 2 times

krzychu3000 1 year, 1 month ago

Selected Answer: D

D, License
upvoted 1 times

zellck 1 year, 3 months ago

Selected Answer: D

D is the answer.

License procurement is not a task that can be automated in Azure DevOps. Procuring licenses requires purchasing licenses through Microsoft or a Microsoft partner, which involves a human decision-making process.
upvoted 3 times

Mcs_ 1 year, 4 months ago

D. License procurement.
Group membership changes, license assignment, and assigning entitlements can all be automated using tools such as Azure DevOps and Azure Active Directory. However, license procurement involves purchasing licenses from a vendor, which typically requires manual intervention.
upvoted 3 times

VlatkoS 1 year, 7 months ago

Right answer is D. Procurement of license cannot be automated.
upvoted 1 times

Cubbywoo 1 year, 7 months ago

D
While the other tasks, such as group membership changes, license assignment, and assigning entitlements can potentially be automated using

Azure DevOps and other tools, license procurement itself is a process that typically involves manual negotiations, agreements, and contracts with vendors.

upvoted 2 times

DarioReymag 1 year, 9 months ago

Also think D is correct

upvoted 1 times

friendlyvlad 1 year, 9 months ago

The answer is D; the rest can be automated either by Group Rules, PowerShell, or DevOps API.

upvoted 4 times

Hg6421 1 year, 10 months ago

Selected Answer: A

Answer is A

upvoted 1 times

Hg6421 1 year, 10 months ago

Sorry for the mistake, it is D

upvoted 3 times

Riahlead 2 years, 1 month ago

Selected Answer: D

Its D . As it cannot be automated required collaboration with vendors

upvoted 2 times

syu31svc 2 years, 1 month ago

Selected Answer: D

This is D for sure

Since when license procurement can be an automated thing anyway?

upvoted 2 times

Govcomm 2 years, 1 month ago

Correct, D, procurement has to done manually.

upvoted 1 times

ccoutinho 2 years, 3 months ago

What is license procurement?

upvoted 1 times

certstowinirl 2 years, 2 months ago

Purchasing on new licenses

upvoted 2 times

Kubernetes 2 years, 4 months ago

D is correct

upvoted 1 times

jay158 2 years, 4 months ago

Selected Answer: A

Modifying group memberships is a manual task. So A is the answer.
https://docs.microsoft.com/en-us/azure/devops/organizations/billing/buy-basic-access-add-users?view=azure-devops

upvoted 3 times

Cyrospawn 2 years, 1 month ago

Group membership/ access can be automated. This information is on the same page of the link you provided. Simply scroll down farther. :-)
https://docs.microsoft.com/en-us/azure/devops/organizations/billing/buy-basic-access-add-users?view=azure-devops#automate-access-with-group-rules

upvoted 3 times

basw77 2 years, 2 months ago

You are right and the linked article explains it well

upvoted 1 times

Question #4 *Topic 1*

You have been tasked with strengthening the security of your team's development process.
You need to suggest a security tool type for the Continuous Integration (CI) phase of the development process.
Which of the following is the option you would suggest?

A. Penetration testing

B. Static code analysis

C. Threat modeling

D. Dynamic code analysis

Suggested Answer: *B*
Validation in the CI/CD begins before the developer commits his or her code. Static code analysis tools in the IDE provide the first line of defense to help ensure that security vulnerabilities are not introduced into the CI/CD process.
Reference:
https://docs.microsoft.com/en-us/azure/devops/articles/security-validation-cicd-pipeline?view=vsts

> **Note**
>
> Azure Pipelines is one among a collection of Azure DevOps Services, all built on the same secure infrastructure in Azure. To understand the main concepts around security for all of Azure DevOps Services, see **Azure DevOps Data Protection Overview** and **Azure DevOps Security and Identity.**

Traditionally, organizations implemented security through draconian lock-downs. Code, pipelines, and production environments had severe restrictions on access and use. In small organizations with a few users and projects, this stance was relatively easy to manage. However, that's not the case in larger organizations. Where many users have contributor access to code, one must "assume breach". Assuming breach means behaving as if an adversary has contributor access to some (if not all) of the repositories.

Community vote distribution

B (100%)

ccoutinho Highly Voted 2 years, 3 months ago
Answer B is correct. However, the explanation is not! Static Code Analysis can be performed in the IDE, but that's not within the scope of the question... Static Code Analysis should be performed in the CI pipeline, so that vulnerabilities are not introduced in the main codebase. Penetration testing and Dynamic code analysis can only be performed over a live environment, and threat modeling is obviously wrong. That is why Static Code Analysis is the correct answer!
upvoted 30 times

ozbonny 6 months, 4 weeks ago
But Static Code Analysis can be implemented like sonarqube and be added as gateway validation in a PR
upvoted 1 times

renzoku Highly Voted 1 year, 2 months ago
Selected Answer: B
B. Static code analysis
You can analyse your source code without executing it(during CI phase), detect security weaknesses before integrate your code to the main source code.

Penetration testing, typically performed after CI/CD processes, identify vulnerabilities and assess the security, simultating real-attacks

Dynamic code analysis, unlike Static code analysis this evaluates the app during runtime (not during CI)

Threat modeling, identifies potential threats and vulnerabilities for the app

upvoted 7 times

[Removed] Most Recent 4 months, 2 weeks ago

Selected Answer: B

Static code analysis (during CI): Analyze code for vulnerabilities early, before it merges into the main codebase.
Penetration testing (after CI/CD): Simulate real attacks to find weaknesses after the application is built.
Dynamic code analysis (during runtime): Continuously assess security while the application is running.
Threat modeling: Proactively identify potential threats and vulnerabilities throughout the development process.
"With the Microsoft Security Code Analysis extension, teams can add security code analysis to their Azure DevOps continuous integration and delivery (CI/CD) pipelines."
Reference Link: https://docs.microsoft.com/en-us/azure/security/develop/security-code-analysis-overview
Thumb Rule: -
For PR: - Static Code Analysis
CI: - Static Code Analysis
CD: - Penetration Testing
For access to all 493 practice questions drop an email at reviewnerd045@gmail.com

upvoted 1 times

kleansoul 1 year ago

Selected Answer: B

CI is where Static Code Analysis can be performed.

upvoted 2 times

krzychu3000 1 year, 1 month ago

Selected Answer: B

Static code analysis

upvoted 1 times

Msds1981 1 year, 1 month ago

Selected Answer: B

Answer is B, static code analysis

upvoted 1 times

igweone 1 year, 2 months ago

The Answer is correct

upvoted 1 times

DarioReymag 1 year, 9 months ago

B pdf page 55

upvoted 1 times

Hg6421 1 year, 10 months ago

Selected Answer: B

Answer is B

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: B

https://docs.microsoft.com/en-us/azure/security/develop/security-code-analysis-overview

"With the Microsoft Security Code Analysis extension, teams can add security code analysis to their Azure DevOps continuous integration and delivery (CI/CD) pipelines"

Answer is B

upvoted 4 times

Govcomm 2 years, 1 month ago

Correct, B, build pipeline static code analysis such as SonarQube.

upvoted 2 times

gt002 2 years, 4 months ago

ANSWER B:
The Best Static Code Analysis Tools
SonarQube. SonarQube sample debugging error message. ...

Checkmarx SAST CxSAST. Checkmarx SAST projects scan. ...
Synopsis Coverity. Synopsis Coverity sample dashboard. ...
Micro Focus Fortify Static Code Analyzer. ...
Veracode Static Analysis. ...
Snyk Code. ...
Reshift Security.
upvoted 3 times

Question #5 *Topic 1*

Your company is currently making use of Team Foundation Server 2013 (TFS 2013), but intend to migrate to Azure DevOps.
You have been tasked with supplying a migration approach that allows for the preservation of Team Foundation Version Control changesets dates, as well as the changes dates of work items revisions. The approach should also allow for the migration of all TFS artifacts, while keeping migration effort to a minimum.
You have suggested upgrading TFS to the most recent RTW release.
Which of the following should also be suggested?

A. Installing the TFS kava SDK

B. Using the TFS Database Import Service to perform the upgrade.

C. Upgrading PowerShell Core to the latest version.

D. Using the TFS Integration Platform to perform the upgrade.

Suggested Answer: *B*
In Phase 3 of your migration project, you will work on upgrading your Team Foundation Server to one of the supported versions for the Database Import Service in
Azure Devops Services.

Community vote distribution

B (100%)

fkaracan Highly Voted 1 year, 7 months ago
Ignore my previous answer. The answer is B :)
upvoted 5 times

Puskar Most Recent 1 year, 6 months ago
This is right
upvoted 1 times

fkaracan 1 year, 7 months ago
Answer is D. Key part here is "keeping the migration effort to minimum and all TFS artifacts".

Using the TFS Integration Platform allows you to migrate all TFS artifacts, including version control history and work items.
upvoted 1 times

DarioReymag 1 year, 9 months ago
D page 151 troubleshooting
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: B
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/migrate/azure-best-practices/contoso-migration-tfs-vsts

"Upgrade the Team Foundation Server implementation to a supported level"

Answer is B
upvoted 4 times

Govcomm 2 years, 1 month ago
Correct, B, upgrade TFS and then perform Database migration tool.
upvoted 1 times

Leandrocei 2 years, 2 months ago
Correct. Came today 22 july 9
upvoted 2 times

Bluepilot02 2 years, 4 months ago
Selected Answer: B
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/migrate/azure-best-practices/contoso-migration-tfs-vsts

upvoted 3 times

Pravanjan 2 years, 4 months ago

Selected Answer: B

Correct!

upvoted 2 times

DRAG DROP -

You have an on-premises Bitbucket Server with a firewall configured to block inbound Internet traffic. The server is used for Git-based source control.

You intend to manage the build and release processes using Azure DevOps. This plan requires you to integrate Azure DevOps and Bitbucket.

Which of the following will allow for this integration? Answer by dragging the correct options from the list to the answer area.

Select and Place:

Options	Answer
A self-hosted agent	
A Microsoft-hosted agent	
An External Git service connection	
Service hooks	

Suggested Answer:

Options	Answer
A self-hosted agent	A self-hosted agent
A Microsoft-hosted agent	An External Git service connection
An External Git service connection	
Service hooks	

Reference:

https://docs.microsoft.com/en-us/azure/devops/pipelines/repos/pipeline-options-for-git

Feature	Azure Pipelines	TFS 2017.2 and higher	TFS 2017 RTM	TFS 2015.4	TFS 2015 RTM
Branch	Yes	Yes	Yes	Yes	Yes
Clean	Yes	Yes	Yes	Yes	Yes
Tag or label sources	Project; Classic only	Team project	Team project	Team project	No
Report build status	Yes	Yes	Yes	No	No
Checkout submodules	Yes	Yes	Yes	Yes	Yes

syu31svc Highly Voted 2 years, 1 month ago
https://docs.microsoft.com/en-us/azure/devops/pipelines/repos/on-premises-bitbucket?view=azure-devops

"This is again probably caused by a firewall blocking traffic from these servers. You have two options in this case:

Switch to using self-hosted agents or scale-set agents"

"Is your Bitbucket server accessible from Azure Pipelines? Azure Pipelines periodically polls Bitbucket server for changes. If the Bitbucket server is behind a firewall, this traffic may not reach your server. See Azure DevOps IP Addresses and verify that you have granted exceptions to all the required IP addresses. These IP addresses may have changed since you have originally set up the exception rules. You can only start manual runs if you used an external Git connection and if your server is not accessible from Azure Pipelines."

Answer is correct
upvoted 9 times

Lucario95 Highly Voted 2 years, 3 months ago
As jay158's answer, Examtopics' answer is correct
upvoted 8 times

FeriAZ Most Recent 6 months, 2 weeks ago
1- Self-hosted agent: This is a software application that you install on a machine within your network (not necessarily the Bitbucket server) to run jobs and tasks for your pipelines in Azure DevOps. It can be used with the External Git service connection to interact with your Bitbucket server without requiring inbound internet access.

2- External Git service connection: This is a configuration in Azure DevOps that allows it to connect to an external Git repository like your on-premises Bitbucket server. It can be used in conjunction with a self-hosted agent to access and interact with your Bitbucket repositories behind the firewall.
upvoted 5 times

ozbonny 6 months, 4 weeks ago
A self-hosted agent: This would allow you to run build and release tasks in a self-controlled environment, which is essential if you can't allow Azure DevOps agents to directly access the Bitbucket server over the internet.
A service connection to an external Git service (external git service connection): This would provide a way to connect to your Bitbucket repository from Azure DevOps without needing to open additional ports on your firewall.
upvoted 1 times

ozbonny 6 months, 4 weeks ago
Un agente autohospedado (self-hosted agent): Esto permitiría ejecutar tareas de compilación y lanzamiento en un entorno controlado por ti mismo, lo que es esencial si no puedes permitir que los agentes de Azure DevOps accedan directamente al servidor Bitbucket a través de Internet.

Una conexión de servicio a un servicio Git externo (external git service connection): Esto proporcionaría una forma de conectarse a tu repositorio Bitbucket desde Azure DevOps sin necesidad de abrir puertos adicionales en tu firewall.
upvoted 1 times

ashfaqbarkati786 8 months, 2 weeks ago
started today, will be back once certification is complete
upvoted 2 times

vsvaid 9 months ago
https://learn.microsoft.com/en-us/azure/devops/pipelines/repos/on-premises-bitbucket?view=azure-devops

Switch to using self-hosted agents or scale-set agents. These agents can be set up within your network and hence will have access to the Bitbucket server. These agents only require outbound connections to Azure Pipelines. There is no need to open a firewall for inbound connections.

Correct Answer
upvoted 1 times

Firdous586 10 months, 3 weeks ago
Given Answer is correct
Service Hooks is not related to this question as per MS Document Defination.
Service hooks let you run tasks on other services when events happen in your project in Azure DevOps. For example, you can create a card in Trello when a work item gets created or send a push notification to your team's mobile devices when a build fails
upvoted 3 times

mct_esteban_calabria 1 year, 3 months ago
I would not choose Service Connection because on premis bitbuket is blocking inbound traffic from internet
upvoted 1 times

zellck 1 year, 3 months ago
1. Self-hosted agent
2. External GIT service connection

https://learn.microsoft.com/en-us/azure/devops/pipelines/repos/on-premises-bitbucket?view=azure-devops#not-reachable-from-microsoft-hosted-agents
Switch to using self-hosted agents or scale-set agents. These agents can be set up within your network and hence will have access to the Bitbucket server. These agents only require outbound connections to Azure Pipelines. There is no need to open a firewall for inbound connections. Make sure that the name of the server you specified when creating the service connection is resolvable from the self-hosted agents.
upvoted 5 times

Mallena 1 year, 8 months ago
yes, it's possible only with self-hosted agent

https://learn.microsoft.com/en-us/azure/devops/pipelines/repos/on-premises-bitbucket?view=azure-devops
upvoted 1 times

DarioReymag 1 year, 9 months ago
searches are wildcards
upvoted 1 times

Jenthika 2 years, 1 month ago
You can integrate your on-premises Bitbucket server or another Git server with Azure Pipelines. Your on-premises server may be exposed to the Internet or it may not be.

If your on-premises server is reachable from the servers that run Azure Pipelines service, then:

you can set up classic build and configure CI triggers
If your on-premises server is not reachable from the servers that run Azure Pipelines service, then:

you can set up classic build pipelines and start manual builds
you cannot configure CI triggers

If your on-premises server is reachable from the hosted agents, then you can use the hosted agents to run manual, scheduled, or CI builds.

Otherwise, you must set up self-hosted agents that can access your on-premises server and fetch the code.

https://docs.microsoft.com/en-us/azure/devops/pipelines/repos/on-premises-bitbucket?view=azure-devops
upvoted 2 times

CS1980 2 years, 1 month ago
Why external Git Service Connection? Since Bitbucket blocks incoming connections, wouldn't setting that up fail (Azure Pipelines shouldn't be able to connect to the on-prem bitbucket which blocks inbound traffic). Just self-hosted agent (deployed on prem) should be sufficient?
upvoted 2 times

Govcomm 2 years, 1 month ago
Correct, self-hosted agent for on-premises and then Git service connection.
upvoted 1 times

Dileep75 2 years, 2 months ago
the inbound traffics are blocked , so the given answer is correct
upvoted 1 times

jay158 2 years, 4 months ago
Answer
A Self-hosted agent
Service hooks
https://docs.microsoft.com/en-us/azure/devops/pipelines/repos/bitbucket?view=azure-devops&tabs=classic#access-to-bitbucket-repositories
upvoted 1 times

jay158 2 years, 4 months ago
Ignore 'Service hooks' it for Bitbucket in cloud.
Examtopics answer is correct
https://docs.microsoft.com/en-us/azure/devops/pipelines/repos/on-premises-bitbucket?view=azure-devops
upvoted 12 times

Omarook 1 year, 5 months ago
Inbound traffic is blocked, for me I will choose only self-managed agents
upvoted 1 times

Question #7 *Topic 1*

You are currently developing a project for a client that will be managing work items via Azure DevOps.
You want to make sure that the work item process you use for the client allows for requirements, change requests, risks, and reviews to be tracked.
Which of the following is the option you would choose?

A. Basic

B. Agile

C. Scrum

D. CMMI

Suggested Answer: *D*
Choose CMMI when your team follows more formal project methods that require a framework for process improvement and an auditable record of decisions. With this process, you can track requirements, change requests, risks, and reviews.
Incorrect Answers:
A. Choose Basic when your team wants the simplest model that uses Issues, Tasks, and Epics to track work.
B. This process works great if you want to track user stories and (optionally) bugs on the Kanban board, or track bugs and tasks on the taskboard.
C. This process works great if you want to track product backlog items (PBIs) and bugs on the Kanban board, or break PBIs and bugs down into tasks on the taskboard.
Reference:
https://docs.microsoft.com/en-us/azure/devops/boards/work-items/guidance/choose-process?view=azure-devops

Community vote distribution

D (100%)

gt002 Highly Voted 2 years, 4 months ago
ANSWER D:
CMMI stand for Capability Maturity Model Integration
The Capability Maturity Model Integration (CMMI) is a model that helps organizations to: Effectuate process improvement. Develop behaviors that decrease risks in service, product, and software development.
upvoted 13 times

Ash111 Highly Voted 3 years, 2 months ago
Given answer is correct
upvoted 8 times

Firdous586 Most Recent 10 months, 3 weeks ago
The CMMI process supports the following work item types (WITs) to plan and track work, tests, feedback, and code review. With different WITs you can track different types of work—such as requirements, change requests, tasks, bugs and more. These artifacts are created when you create a project using the CMMI process
upvoted 1 times

zellck 1 year, 3 months ago
Selected Answer: D
D is the answer.

https://learn.microsoft.com/en-us/azure/devops/boards/work-items/guidance/cmmi-process?view=azure-devops
The CMMI process supports the following work item types (WITs) to plan and track work, tests, feedback, and code review. With different WITs you can track different types of work—such as requirements, change requests, tasks, bugs and more. These artifacts are created when you create a project using the CMMI process. They're based on the Capability Maturity Model Integration (CMMI) process.
upvoted 3 times

nhannn 1 year, 10 months ago
Selected Answer: D
D is the correct answer. You can easily see that when creating a project as CMMI process. There are 10 work items available: Bug, Change Request, Epic, Feature, Issue, Requirement, Review, Risk, Task, and Test Case.

upvoted 2 times

Hg6421 1 year, 10 months ago

Selected Answer: D

D is correct

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: D

https://docs.microsoft.com/en-us/azure/devops/boards/work-items/guidance/media/alm_pt_cmmi_wit_artifacts.png?view=azure-devops

Answer is D

upvoted 1 times

Govcomm 2 years, 1 month ago

Correct, CMMI. Scrum is about product backlog and Agile is about the user stories.

upvoted 2 times

Pravanjan 2 years, 4 months ago

Selected Answer: D

Correct!

upvoted 3 times

rdemontis 2 years, 5 months ago

Selected Answer: D

correct

upvoted 1 times

AlMargoi 2 years, 9 months ago

Correct

upvoted 1 times

Question #8 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
You run the Register-AzureRmAutomationDscNode command in your company's environment.
You need to make sure that your company's test servers remain correctly configured, regardless of configuration drift.
Solution: You set the -ConfigurationMode parameter to ApplyOnly.
Does the solution meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/register-azurermautomationdscnode?view=azurermps-6.13.0

Register-AzureRmAutomationDscNode

Module: AzureRM.Automation

Registers an Azure virtual machine as a DSC node for an Automation account.

Important

Because Az PowerShell modules now have all the capabilities of AzureRM PowerShell modules and more, we'll retire AzureRM PowerShell modules on 29 February 2024.

To avoid service interruptions, **update your scripts** that use AzureRM PowerShell modules to use Az PowerShell modules by 29 February 2024. To automatically update your scripts, follow the **quickstart guide**.

Community vote distribution

B (100%)

syu31svc Highly Voted 2 years, 1 month ago

Selected Answer: B

https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/register-azurermautomationdscnode?view=azurermps-6.13.0

Specifies the DSC configuration mode. Valid values are:

ApplyAndMonitor
ApplyAndAutocorrect
ApplyOnly

Answer is No; use ApplyAndAutocorrect for "correctly configured, regardless of configuration drift"
upvoted 18 times

FeriAZ Most Recent 6 months, 2 weeks ago

1. ApplyOnly:

Applies the configuration script once during registration.
Does not monitor for future changes or drift.
Not suitable for situations where continuous configuration management is required.
2. ApplyAndMonitor:

Applies the configuration script initially.

Continuously monitors the registered node for any configuration changes.
If drift is detected, the script is automatically reapplied to bring the node back to the desired state.
Suitable for situations where continuous configuration management is essential to prevent drift and ensure consistent configuration across nodes.
3. ApplyAndAutocorrect:

Applies the configuration script initially.
Continuously monitors the registered node for any configuration changes.
If drift is detected, the script is automatically reapplied to correct the configuration immediately.
Similar to ApplyAndMonitor, but with immediate correction of any drift.
upvoted 1 times

ozbonny 6 months, 4 weeks ago
The proposed solution sets the -ConfigurationMode parameter to ApplyOnly when running the Register-AzureRmAutomationDscNode command. This indicates that the configuration will only be applied, but will not be checked or corrected for any configuration deviation (drift).

Since the goal is to ensure that the company's test servers remain correctly configured regardless of configuration drift, the solution falls short of the goal. The settings will only be applied once and will not be maintained if there are unauthorized changes.

Therefore, the correct answer is B. No.
upvoted 1 times

74gjd_37 1 year ago
Selected Answer: B
https://learn.microsoft.com/en-us/powershell/dsc/managing-nodes/metaconfig?view=dsc-1.1

"ApplyOnly: DSC applies the configuration and does nothing further unless a new configuration is pushed to the target node or when a new configuration is pulled from a service. After initial application of a new configuration, DSC does not check for drift from a previously configured state. Note that DSC will attempt to apply the configuration until it is successful before ApplyOnly takes effect. "
upvoted 1 times

zellck 1 year, 3 months ago
Selected Answer: B
B is the answer.

https://learn.microsoft.com/en-us/powershell/dsc/managing-nodes/metaconfig?view=dsc-1.1#basic-settings
ApplyOnly: DSC applies the configuration and does nothing further unless a new configuration is pushed to the target node or when a new configuration is pulled from a service. After initial application of a new configuration, DSC does not check for drift from a previously configured state.
upvoted 3 times

sca88 1 year, 3 months ago
https://learn.microsoft.com/en-us/powershell/dsc/managing-nodes/metaconfig?view=dsc-1.1
upvoted 1 times

nhannn 1 year, 10 months ago
Selected Answer: B
It's B - No. With ApplyOnly: After the initial application of a new configuration, DSC does not check for drift from a previously configured state.

It should be ApplyAndAutocorrect
upvoted 3 times

rods 1 year, 11 months ago
Selected Answer: B
Correct answer!
upvoted 2 times

bishtr3 2 years ago
Answer B
This link beautifully explained DSC configuration mode
https://www.red-gate.com/simple-talk/sysadmin/powershell/powershell-desired-state-configuration-the-basics/
upvoted 1 times

reynaldo_aguiar 2 years ago

Selected Answer: B

Answer B

https://tkolber.medium.com/configuring-azure-dsc-automation-with-powershell-in-5-steps-454fbef9457b

upvoted 1 times

Govcomm 2 years, 1 month ago

No, ApplyAndAutocorrect is the right answer.

upvoted 1 times

UnknowMan 2 years, 4 months ago

Right , the option is ApplyAndAutocorrect

upvoted 4 times

Question #9 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result.
Establish if the solution satisfies the requirements.
You run the Register-AzureRmAutomationDscNode command in your company's environment.
You need to make sure that your company's test servers remain correctly configured, regardless of configuration drift.
Solution: You set the -ConfigurationMode parameter to ApplyAndMonitor.
Does the solution meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/register-azurermautomationdscnode?view=azurermps-6.13.0

Community vote distribution

B (100%)

nhannn Highly Voted 1 year, 10 months ago

Selected Answer: B

It's B - No. With ApplyAndMonitor: After the initial application of a new configuration, if the target node drifts from the desired state, DSC reports the discrepancy in logs.

It should be ApplyAndAutocorrect

upvoted 5 times

ozbonny Most Recent 6 months, 4 weeks ago

ApplyAndMonitor: The configuration is applied and checked periodically. If a change is noticed, then an entry is created in the event log.

The proposed solution sets the -ConfigurationMode parameter to ApplyOnly when running the Register-AzureRmAutomationDscNode command. This indicates that the configuration will only be applied, but will not be checked or corrected for any configuration deviation (drift).

Since the goal is to ensure that the company's test servers remain correctly configured regardless of configuration drift, the solution falls short of the goal. The settings will only be applied once and will not be maintained if there are unauthorized changes.

Therefore, the correct answer is B. No.

upvoted 1 times

74gjd_37 1 year ago

Selected Answer: B

https://learn.microsoft.com/en-us/powershell/dsc/managing-nodes/metaconfig?view=dsc-1.1

ApplyAndMonitor: This is the default value. The LCM applies any new configurations. After initial application of a new configuration, if the target node drifts from the desired state, DSC reports the discrepancy in logs. Note that DSC will attempt to apply the configuration until it is successful before ApplyAndMonitor takes effect.

upvoted 1 times

zellck 1 year, 3 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/powershell/dsc/managing-nodes/metaconfig?view=dsc-1.1#basic-settings
ApplyAndMonitor: This is the default value. The LCM applies any new configurations. After initial application of a new configuration, if the target node drifts from the desired state, DSC reports the discrepancy in logs.

upvoted 2 times

DarioReymag 1 year, 9 months ago

D page 151 troubleshooting

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: B

https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/register-azurermautomationdscnode?view=azurermps-6.13.0

Specifies the DSC configuration mode. Valid values are:

ApplyAndMonitor
ApplyAndAutocorrect
ApplyOnly

Answer is No; use ApplyAndAutocorrect for "correctly configured, regardless of configuration drift"

upvoted 4 times

Govcomm 2 years, 1 month ago

No, ApplyAndAutocorrect is the right answer.

upvoted 1 times

UnknowMan 2 years, 4 months ago

Selected Answer: B

ApplyAndAutocorrect Do The job

upvoted 4 times

rdemontis 2 years, 5 months ago

Selected Answer: B

correct answer. ApplyAndMonitor doesn't change the state of the machine if there is a deviation from initial configuration. It only logs the activity

upvoted 4 times

d0bermannn 2 years, 12 months ago

ApplyAndAutocorrect option is all that we need there, just see get-help Register-AzAutomationDscNode

upvoted 4 times

fabulousethiopia 3 years, 1 month ago

ApplyAndMonitor: ..After initial application of a new configuration, if the target node drifts from the desired state, DSC reports the discrepancy in logs. Note that DSC will attempt to apply the configuration until it is successful before ApplyAndMonitor takes effect.

upvoted 1 times

ScreamingHand 3 years, 1 month ago

ApplyAndMonitor: The Local Configuration Manager applies any new configurations. After initial application of a new configuration, if the target node drifts from the desired state, DSC reports the discrepancy in logs.

upvoted 2 times

ZodiaC 3 years, 2 months ago

Correct

upvoted 1 times

Question #10 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
You run the Register-AzureRmAutomationDscNode command in your company's environment.
You need to make sure that your company's test servers remain correctly configured, regardless of configuration drift.
Solution: You set the -ConfigurationMode parameter to ApplyAndAutocorrect.
Does the solution meet the goal?

A. Yes

B. No

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/register-azurermautomationdscnode?view=azurermps-6.13.0

Community vote distribution

A (100%)

VamshiJupelli Highly Voted 2 months, 2 weeks ago
Got this question in my exam on 17 June 2024. Scored 813, Passing score 700

There were 41 normal questions, 2 case studies with 5 questions in each, and 1 lab set with 12 tasks. Including the lab, about 40% of the questions were new to me, given I didn't purchase the full version of dumps from any website.

The lab was all about Azure DevOps rather than Azure Portal, like making a service connection, setting up branch policies, adding a .NET build task, docker deploy task, setting up an agent pool, creating an artifact feed, setting up pull request triggers etc. I was able to do 9 out of 12.

All the best!
upvoted 5 times

ozbonny Most Recent 6 months, 4 weeks ago
ApplyAndAutocorrect: The configuration is applied and the LCM verifies periodically that there is no variation. If a change is noticed, then the configuration is reapplied.

Then Correct Answer
upvoted 1 times

zellck 1 year, 3 months ago
Selected Answer: A
A is the answer.

https://learn.microsoft.com/en-us/powershell/dsc/managing-nodes/metaconfig?view=dsc-1.1#basic-settings
ApplyAndAutoCorrect: DSC applies any new configurations. After initial application of a new configuration, if the target node drifts from the desired state, DSC reports the discrepancy in logs, and then re-applies the current configuration.
upvoted 3 times

nhannn 1 year, 10 months ago
Selected Answer: A
It's A - Yes. With ApplyAndAutocorrect: DSC applies any new configurations. After initial application of a new configuration, if the target node drifts from the desired state, DSC reports the discrepancy in logs, and then re-applies the current configuration
upvoted 4 times

Hg6421 1 year, 10 months ago
Selected Answer: A
Right answer is A
upvoted 2 times

syu31svc 2 years, 1 month ago

Selected Answer: A

https://docs.microsoft.com/en-us/powershell/module/azurerm.automation/register-azurermautomationdscnode?view=azurermps-6.13.0

Specifies the DSC configuration mode. Valid values are:

ApplyAndMonitor
ApplyAndAutocorrect
ApplyOnly

Answer is Yes; use ApplyAndAutocorrect for "correctly configured, regardless of configuration drift"

upvoted 2 times

Govcomm 2 years, 1 month ago

Yes, ApplyAndAutocorrect is the right answer for the configuration drift.

upvoted 1 times

kennynelcon 2 years, 1 month ago

Selected Answer: A

ApplyandAutoCorrect is accurate

upvoted 2 times

UnknowMan 2 years, 4 months ago

Selected Answer: A

correct

upvoted 3 times

rdemontis 2 years, 5 months ago

Selected Answer: A

correct answer

upvoted 3 times

d0bermannn 2 years, 12 months ago

ApplyAndAutocorrect option is all that we need there, just see get-help Register-AzAutomationDscNode

upvoted 3 times

fabulousethiopia 3 years, 1 month ago

ApplyAndAutoCorrect: DSC applies any new configurations. After initial application of a new configuration, if the target node drifts from the desired state, DSC reports the discrepancy in logs, and then re-applies the current configuration.

upvoted 1 times

ScreamingHand 3 years, 1 month ago

ApplyAndAutocorrect is correct, - you can specify how often LCM checks the nodes

upvoted 1 times

jojom19980 3 years, 1 month ago

you can specify that the state of the machine is to be applied only once by specifying ApplyOnly as the value of the ConfigurationMode property. State Configuration doesn't try to apply the configuration after the initial check.

upvoted 1 times

ZodiaC 3 years, 2 months ago

Its satisfies the requirements, so its correct.

upvoted 4 times

Question #11 *Topic 1*

You need to consider the underlined segment to establish whether it is accurate.
To compile an Internet Information Services (IIS) web application that runs docker, you should use a Default build agent pool.
Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required.

B. Hosted Windows Container

C. Hosted

D. Hosted macOS

Suggested Answer: *C*
Hosted pool (Azure Pipelines only): The Hosted pool is the built-in pool that is a collection of Microsoft-hosted agents.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/v2-osx

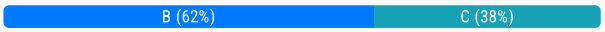
To build and deploy Xcode apps or Xamarin.iOS projects, you'll need at least one macOS agent. This agent can also build and deploy Java and Android apps.

> Before you begin:
>
> - If your pipelines are in Azure Pipelines and a Microsoft-hosted agent meets your needs, you can skip setting up a self-hosted macOS agent.
> - Otherwise, you've come to the right place to set up an agent on macOS. Continue to the next section.

Learn about agents

If you already know what an agent is and how it works, feel free to jump right in to the following sections. But if you'd like some more background about what they do and how they work, see Azure Pipelines agents.

Community vote distribution



esend3 Highly Voted 2 years, 4 months ago
Selected Answer: B
Should be the answer
upvoted 28 times

Rams_84zO6n 1 year, 6 months ago
esend3, do you actually see the underlined text on the questions? For me it doesn't render correctly. I use chrome browser on a macbook pro. Any advise?
upvoted 5 times

AzureJobsTillRetire Highly Voted 1 year, 8 months ago
Selected Answer: C
The question asks if you "should use a Default build agent pool", with the word "Default" highlighted. The word "Default" can be replaced with "Hosted", which gives us the answer C.

If the question asks for if you "should use a Default Build Agent Pool", the answer should be B (Hosted Windows Container)
upvoted 13 times

Shadoken Most Recent 4 months, 2 weeks ago
The underlined segment is inaccurate. To compile an Internet Information Services (IIS) web application that runs on Docker, the appropriate build agent pool to use would be a Hosted Windows Container pool. This pool provides a Windows environment with Docker support to ensure that the application is built and run in the appropriate environment.

So the correct option is: B. Hosted Windows Container (Answered by Copilot)
upvoted 1 times

4bd3116 4 months, 4 weeks ago

Selected Answer: B

IIS (Internet Information Services) is a web server software designed by Microsoft and is primarily built for the Windows operating system. It is not natively supported on macOS. Therefore, if you need to compile an IIS web application, you would typically require a Windows-based environment.
upvoted 1 times

chloaus 5 months, 2 weeks ago

B.
https://medium.com/@walissonscd/build-agent-pools-for-dockerized-iis-web-applications-choosing-the-right-option-21b86c097436
upvoted 1 times

FeriAZ 6 months, 2 weeks ago

Selected Answer: B

B. Hosted Windows Container: This type of agent pool specifically provides Windows agents with Docker pre-installed and configured, making them suitable for building Dockerized applications, including IIS web apps.
upvoted 2 times

Alex1998 6 months, 1 week ago

Hey, do you know if now in the exam are still availables the labs?
upvoted 1 times

ozbonny 6 months, 4 weeks ago

I think I'll go with Hosted Windows Container because of the following:
Reasoning:

The Azure DevOps Hosted build agent pool contains a variety of agents with different operating systems, including Windows.
Some of the Windows agents in the pool support Docker.
IIS is a Windows web server.
Therefore, it is logical to deduce that the "Hosted build agent pool" contains agents that can run IIS web applications with Docker.

However, it is important to note that not all Windows agents in the pool support Docker.

To ensure compatibility, it is recommended:

Select a Windows agent that is labeled "Docker" in the agent list.
upvoted 1 times

uncledana 8 months, 2 weeks ago

C is the answer - the specifics of the application isn't mentioned, therefore using the 'hosted' is the default
upvoted 1 times

vsvaid 8 months, 3 weeks ago

Selected Answer: C

I think C, hosted pool is correct
upvoted 1 times

son_el 9 months, 3 weeks ago

the answer is b cause iis is created only to run on windows
upvoted 1 times

Firdous586 10 months, 3 weeks ago

Azure Pipelines can run Linux or Windows Containers. Use either hosted Ubuntu for Linux containers, or the Hosted Windows Container pool for Windows containers. (The Hosted macOS pool doesn't support running containers.)

When you need to compile an Internet Information Services (IIS) web application that runs on Docker, you should use a Hosted Windows Container build agent pool. This is because IIS is a web server created by Microsoft specifically for Windows-based systems. Since you want to run the application in a Docker container, a Hosted Windows Container build agent pool will provide the necessary Windows environment along with Docker support.

Reference:
https://learn.microsoft.com/en-us/azure/devops/pipelines/process/service-containers?view=azure-devops&tabs=yaml#requirements
upvoted 3 times

kleansoul 12 months ago

Selected Answer: B

The answer should be Hosted Windows Container.

https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/docker?view=azure-devops
upvoted 2 times

AymanAkk 1 year ago

Selected Answer: B

answer is B
upvoted 1 times

irene25_ 1 year ago

Selected Answer: B

IIS web applications can only run on Windows
upvoted 2 times

yana_b 1 year, 1 month ago

Selected Answer: C

Correct answer is C
The agent pool could be either MS hosted or self-hosted.
In regard with self hosted -> You can install the agent on Linux, macOS, or Windows machines. You can also install an agent on a Docker container. For more information about installing a self-hosted agent, see:
- macOS agent
- Linux agent
- Windows agent
- Docker agent
https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/agents?view=azure-devops&tabs=browser
upvoted 2 times

yana_b 11 months ago

Correct answer is B as we speak about running Docker.
upvoted 1 times

itexamsmicrosoft 1 year, 2 months ago

Selected Answer: B

The best answer is:
B. Hosted Windows Container
Explanation:
When compiling an Internet Information Services (IIS) web application that runs Docker, you should use an agent pool that supports Docker and is also based on Windows, since IIS is a Windows service. In Azure DevOps, the "Hosted Windows Container" agent pool is equipped to handle Docker containers and is particularly suited for Windows-based containers.
"Hosted Windows Container" is the most appropriate choice for compiling a Docker-based IIS web application.
upvoted 4 times

fishy_resolver 1 year, 2 months ago

Selected Answer: C

Based on Microsoft's documentation you don't need a container to build a container, you do need a Microsoft-hosted Windows agents or Windows platform based self-hosted agents.
https://learn.microsoft.com/en-us/azure/devops/pipelines/ecosystems/containers/build-image?view=azure-devops
upvoted 3 times

Question #12 *Topic 1*

Your company has an Azure DevOps environment that can only be accessed by Azure Active Directory users.
You are instructed to make sure that the Azure DevOps environment can only be accessed from devices connected to the company's on-premises network.
Which of the following actions should you take?

A. Assign the devices to a security group.

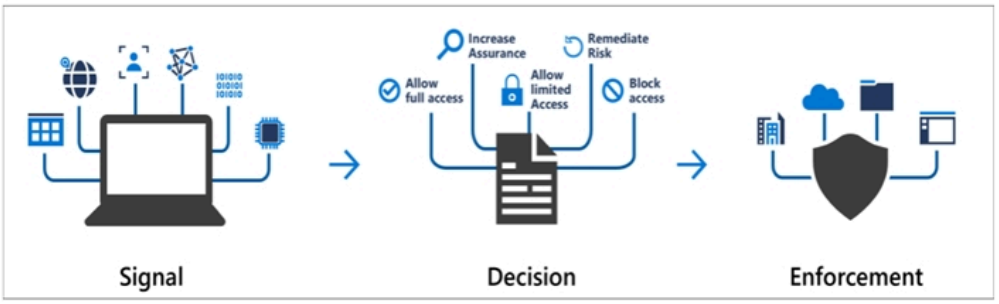
B. Create a GPO.

C. Configure Security in Project Settings from Azure DevOps.

D. Configure conditional access in Azure Active Directory.

Suggested Answer: *D*
Conditional Access is a capability of Azure Active Directory. With Conditional Access, you can implement automated access control decisions for accessing your cloud apps that are based on conditions.
Conditional Access policies are enforced after the first-factor authentication has been completed.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Conditional Access is the tool used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies. Conditional Access is at the heart of the new identity driven control plane.



Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action. Example: A payroll manager wants to access the payroll application and is required to perform multi-factor authentication to access it.

Administrators are faced with two primary goals:

Community vote distribution

D (100%)

Yindave 4 months, 3 weeks ago
I mean... Yes its D, i gto it correct as i've done the AZ-104, but isnt this much more an AZ-104 question then a DevOps question?
upvoted 1 times

FeriAZ 6 months, 2 weeks ago
Selected Answer: D
D. Configure conditional access in Azure Active Directory: This is the correct option. Azure AD conditional access allows you to define granular access policies based on various factors, including the user's identity, device attributes (such as location), and other conditions. By creating a conditional access policy that requires devices to be connected to the company's on-premises network for accessing the Azure DevOps environment, you can achieve the desired location-based access control.
upvoted 2 times

yana_b 1 year, 1 month ago
Selected Answer: D
Correct answer is D
upvoted 2 times

elmarkos23 1 year, 2 months ago

Selected Answer: D

In summary, to ensure that Azure DevOps can only be accessed from devices connected to the company's on-premises network, the recommended action is to configure conditional access in Azure Active Directory (option D).

upvoted 1 times

zellck 1 year, 3 months ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/devops/release-notes/roadmap/conditional-access-policy

upvoted 3 times

Hg6421 1 year, 10 months ago

Selected Answer: D

D is the answer

upvoted 2 times

syu31svc 2 years, 1 month ago

Selected Answer: D

"can only be accessed from devices connected to the company's on-premises network"

Conditional access so D is the answer

upvoted 1 times

Govcomm 2 years, 1 month ago

Azure AD Conditional Access is the answer to block the access from the certain IP range.

upvoted 2 times

UnknowMan 2 years, 4 months ago

Selected Answer: D

correct

upvoted 3 times

Eltooth 2 years, 4 months ago

Selected Answer: D

D is correct answer.

upvoted 1 times

dupakonia 2 years, 4 months ago

correct

upvoted 1 times

esend3 2 years, 4 months ago

Selected Answer: D

Correct

upvoted 1 times

DoctorCOmputer 2 years, 4 months ago

Correct!

https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal?msclkid=1506015dc14c11eca871a7d1f7efcb35

Important

We recommend that you use the Register or join devices user action in Conditional Access to enforce multifactor authentication for joining or registering a device.
You must configure this setting to No if you're using Conditional Access policy to require multifactor authentication.

upvoted 2 times

Question #13 *Topic 1*

You are making use of Azure DevOps to configure Azure Pipelines for project, named PROJ-01.
You are preparing to use a version control system that allows for source code to be stored on a managed Windows server located on the company network.
Which of the following is the version control system you should use?

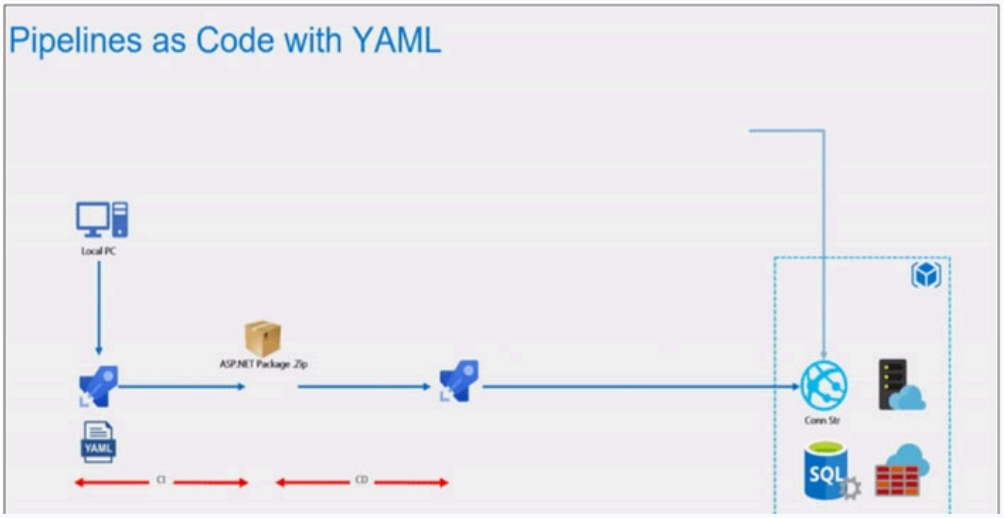
A. Github Enterprise

B. Bitbucket cloud

C. Github Professional

D. Git in Azure Repos

Suggested Answer: *A*
GitHub Enterprise is the on-premises version of GitHub.com. GitHub Enterprise includes the same great set of features as GitHub.com but packaged for running on your organization's local network. All repository data is stored on machines that you control, and access is integrated with your organization's authentication system (LDAP, SAML, or CAS).
Reference:
https://www.azuredevopslabs.com/labs/azuredevops/yaml/



https://enterprise.github.com/faq

Community vote distribution

A (83%) D (17%)

syu31svc Highly Voted 2 years, 1 month ago

Selected Answer: A

GitHub Enterprise is the on-premises version of GitHub.com. GitHub Enterprise includes the same great set of features as GitHub.com but packaged for running on your organization's local network. All repository data is stored on machines that you control, and access is integrated with your organization's authentication system (LDAP, SAML, or CAS).

Answer is A

upvoted 9 times

vLabz Most Recent 11 months, 1 week ago

Selected Answer: D

Azure Repos exists in Azure DevOps Server (on prem)
Question does not talk about Azure DevOps Service, it only mentions Azure DevOps.
Github Enterprise runs on Linux.
Azure DevOps is the only possible solution.

upvoted 2 times

cluqueg 10 months, 3 weeks ago

Github could also be installed on Windows with Hyper-X
https://docs.github.com/en/enterprise-server@3.6/admin/installation/setting-up-a-github-enterprise-server-instance/installing-github-

enterprise-server-on-hyper-v.
Moreover, Azure DevOps server could work as well:
https://learn.microsoft.com/en-us/azure/devops/server/install/single-server?view=azure-devops-2022
upvoted 3 times

kiko90909 1 month, 1 week ago
to store source code on a managed Windows server located on the company network, the best choice would be D. Git in Azure Repos. Azure Repos is integrated with Azure DevOps and allows you to host your repositories on your own infrastructure, providing the control and security you need.
upvoted 1 times

BayleafSoftware 11 months, 1 week ago
Selected Answer: D
Git in Azure Repos
as stated, the question says "Windows" servers.
upvoted 2 times

Gabe_name 1 year ago
The answer is not GitHub enterprise. GHES can only be run on Linux
https://docs.github.com/en/enterprise-server@3.8/admin/overview/about-github-enterprise-server
upvoted 3 times

yana_b 1 year, 1 month ago
Selected Answer: A
Correct answer is Github Enterprise
upvoted 1 times

zellck 1 year, 3 months ago
Selected Answer: A
A is the answer.

https://docs.github.com/en/enterprise-server@3.8/admin/overview/about-github-enterprise-server#about-github-enterprise-server
GitHub Enterprise Server is a self-hosted platform for software development within your enterprise. Your team can use GitHub Enterprise Server to build and ship software using Git version control, powerful APIs, productivity and collaboration tools, and integrations. Developers familiar with GitHub.com can onboard and contribute seamlessly using familiar features and workflows.
upvoted 2 times

gam19 1 year, 5 months ago
I don't get it how the picture relates to the question and answer... any comments?
upvoted 1 times

charlilec 1 year, 5 months ago
chatgpt:
The version control system you should use is D. Git in Azure Repos.

Git in Azure Repos is a version control system provided by Azure DevOps that allows you to store and manage source code on a managed Windows server located on the company network. It provides a secure and scalable solution for version control that can be integrated with Azure Pipelines for continuous integration and delivery.

Github Enterprise and Github Professional are versions of Github that are installed and hosted on-premises, but they are not provided by Azure DevOps. Bitbucket cloud is a hosted version control system provided by Atlassian, not by Azure DevOps. While these systems may be suitable for version control, they are not the recommended option for use with Azure Pipelines and Azure DevOps.
upvoted 1 times

rahy2k 1 year, 5 months ago
Azure Repos can be Azure DevOps Server(on-prem) as well as Azure DevOps Service(Cloud
) ambiguity is there.A. Git Enterprise is correct only on-premise.
upvoted 1 times

FarEl 1 year ago
Git Enterprise runs on Linux, not Windows. I think the answer is Git in Azure Repos.
https://docs.github.com/en/enterprise-server@3.10/admin/overview/system-overview
upvoted 1 times

Govcomm 2 years, 1 month ago

Git Enterprise supports hosting source code on premises.

upvoted 2 times

Eltooth 2 years, 4 months ago

Selected Answer: A

A is correct answer.

upvoted 3 times

Pravanjan 2 years, 4 months ago

Selected Answer: A

Correct!

upvoted 3 times

dupakonia 2 years, 4 months ago

correct

upvoted 4 times

Question #14 *Topic 1*

You need to consider the underlined segment to establish whether it is accurate.
When moving to Azure DevOps, JIRA must be replaced with the build pipelines Azure DevOps service.
Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required.

B. repos

C. release pipelines

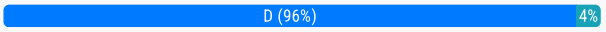
D. boards

Suggested Answer: *C*
Atlassian's Jira Software is a popular application that helps teams to plan, track, and manage software releases, whereas Octopus Deploy helps teams automate their development and operations processes in a fast, repeatable, and reliable manner. Together, they enable teams to get better end-to-end visibility into their software pipelines from idea to production.
Reference:
https://octopus.com/blog/octopus-jira-integration

> Building great software often requires using multiple tools and services, but finding the right ones and getting them to talk to each other can be a headache. Atlassian's Jira Software is a popular application that helps teams to plan, track, and manage software releases, whereas Octopus Deploy helps teams automate their development and operations processes in a fast, repeatable, and reliable manner. Together, they enable teams to get better end-to-end visibility into their software pipelines from idea to production.
>
> Integrating Octopus and Jira Software unlocks three key scenarios:
>
> - See when features or bug fixes are deployed to Prod. "Done" means deployed to production, and this is now visible directly in your Jira issues. See when your team finishes a new feature or bug fix and deploys it to production.

https://www.azuredevopslabs.com/labs/vstsextend/jenkins/

Community vote distribution



Riahlead Highly Voted 2 years, 1 month ago
Selected Answer: D
Jira is task management tool can be replaced with Azure boards which fulfills similar goals
upvoted 34 times

badaboom Highly Voted 1 year, 9 months ago
Selected Answer: D
The correct answer is D, boards.

JIRA is a tool for agile project management, while Azure DevOps is a set of development tools, services, and features that enable teams to plan, develop, deliver, and maintain software more efficiently. While Azure DevOps does include a build pipelines service, it is not a replacement for JIRA. Instead, Azure DevOps has a feature called Azure Boards, which is a tool for agile project management similar to JIRA.

Azure Repos is a version control system that is part of Azure DevOps, and Azure Release Pipelines is a service for creating and managing automated release pipelines for your applications. However, neither of these is a replacement for JIRA.

Therefore, the statement "When moving to Azure DevOps, JIRA must be replaced with the build pipelines Azure DevOps service" is not accurate, and the correct answer is D, boards.
upvoted 8 times

Ansh92 Most Recent 1 month, 3 weeks ago
Selected Answer: D
Azure boards fulfill the JIRA goals.
upvoted 1 times

4bd3116 4 months, 4 weeks ago

Selected Answer: D

When transitioning to Azure DevOps, JIRA should be substituted with Azure DevOps Boards for managing project tasks and workflows.

upvoted 2 times

virnay1 6 months, 4 weeks ago

Azure Boards is the correct answer. JIRA is not comparable to Azure Repos

upvoted 2 times

Thieske 8 months, 3 weeks ago

Misleading question, you don't have to replace Jira as it works fine with Azure DevOps.

upvoted 3 times

Thieske 8 months, 3 weeks ago

The question should be "What is the Azure DevOps equivalent of Jira?". That would be Azure Boards.

upvoted 2 times

kleansoul 12 months ago

Selected Answer: D

Jira is used for managing project tasks. Therefore the correct answer is Azure Boards is the replacement for JIRA.

upvoted 1 times

yana_b 1 year, 1 month ago

Selected Answer: D

It should be D as Jira is a task management tool that helps teams plan, track, and discuss work across the entire software development process. AZ Boards provides a range of features and integrations to help teams collaborate and stay organized with dashboards, reports, and notifications https://learn.microsoft.com/en-us/azure/devops/boards/get-started/what-is-azure-boards?view=azure-devops

upvoted 1 times

stai 1 year, 1 month ago

The correct answer is D, boards.

upvoted 1 times

Vaibhab 1 year, 1 month ago

Correct answer is D, build pipelines are created in jenkins

upvoted 2 times

Msds1981 1 year, 1 month ago

Selected Answer: D

The answer is D for sure, the Azure Boards is a task management tool as well as JIRA.

upvoted 2 times

itexamsmicrosoft 1 year, 2 months ago

Selected Answer: D

answer is d

upvoted 1 times

elmarkos23 1 year, 2 months ago

Selected Answer: D

While Azure DevOps does offer build pipelines and release pipelines for continuous integration and continuous deployment (CI/CD), they are not the direct replacement for JIRA. Instead, the "boards" service in Azure DevOps provides functionality similar to JIRA's project management features, allowing teams to track and manage their work items, tasks, and progress.

Therefore, the accurate option to replace JIRA in the context of Azure DevOps would be the "boards" service.

upvoted 1 times

zellck 1 year, 3 months ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/devops/boards/get-started/what-is-azure-boards?view=azure-devops
Azure Boards is a standalone service within the Azure DevOps suite that helps teams plan, track, and discuss work across the entire software development process. It provides a flexible, customizable platform for managing work items, such as user stories, bugs, tasks, and issues, so you can track your work item's progress throughout the development lifecycle.

Azure Boards supports agile methodologies, including Scrum and Kanban. It provides a range of features and integrations to help teams collaborate and stay organized with dashboards, reports, and notifications.

upvoted 3 times

Singii 1 year, 5 months ago

Selected Answer: D

The underline part should be "build pipelines" thus the answer should be "Boards"

upvoted 1 times

nealjobs 1 year, 6 months ago

it depends on which is the underlined part.

jira vs. board

upvoted 1 times

supercybersecopswarrior 1 year, 6 months ago

Selected Answer: D

JIRA is a task management tool.

A RELEASE is a construct that holds a versioned set of artifacts specified in a CI/CD pipeline.

upvoted 1 times

Question #15 *Topic 1*

You scan a Node.js application using WhiteSource Bolt.
The scan finds numerous libraries with invalid licenses, but are only used during development.
You have to make sure that only production dependencies are scanned by WhiteSource Bolt.
Which of the following is a command you should run?

A. npm edit

B. npm publish

C. npm install

D. npm update

Suggested Answer: *C*
Reference:
https://whitesource.atlassian.net/wiki/spaces/WD/pages/34209870/NPM+Plugin https://nodejs.org/en/knowledge/getting-started/npm/what-is-the-file-package-json

Community vote distribution

C (100%)

jojom19980 Highly Voted 3 years, 1 month ago
The npm install command will install the devDependencies along other dependencies when run inside a package directory, in a development environment (the default).

Use npm install --only=prod (or --only=production) to install only dependencies, and not devDependencies,regardless of the value of the NODE_ENV environment variable.

https://stackoverflow.com/questions/9268259/how-do-you-prevent-install-of-devdependencies-npm-modules-for-node-js-package
upvoted 42 times

Sant25 2 years, 11 months ago
GIVEN ANS CORRECT
npm install will install both "dependencies" and "devDependencies"

npm install --production will only install "dependencies"

npm install --dev will only install "devDependencies"
upvoted 12 times

somenick Highly Voted 1 year, 7 months ago
Just FYI WhiteSource Bolt is now Mend Bolt
upvoted 10 times

FeriAZ Most Recent 6 months, 2 weeks ago
Selected Answer: C
WhiteSource Bolt: Scans your application for vulnerabilities, including those in libraries with invalid licenses.
Scenario: You want to scan only production dependencies, excluding development libraries identified by WhiteSource Bolt.
Correct Command: npm install --only=production (or --only=prod)
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: C
Correct answer is npm install
upvoted 1 times

PravinDhote 1 year, 8 months ago
Selected Answer: C
C is correct
upvoted 1 times

SOMINAZURE 1 year, 9 months ago

C is correct answer.

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: C

C to me

You have to install it so that WhiteSource can scan right?

upvoted 2 times

Govcomm 2 years, 1 month ago

Correct, npm install -production.

upvoted 1 times

Eltooth 2 years, 3 months ago

Selected Answer: C

C is correct answer.

upvoted 3 times

rdemontis 2 years, 5 months ago

Selected Answer: C

correct

https://docs.npmjs.com/cli/v8/commands/npm-install

upvoted 5 times

AlMargoi 2 years, 9 months ago

Correct

upvoted 2 times

Aamir1234 3 years, 1 month ago

correct !

upvoted 3 times

Question #16 *Topic 1*

You are currently defining a release strategy for an app, named APP-01.
The strategy should allow you to keep the time it takes to deploy new releases of the app to a minimum. The strategy should also allow you to roll back in the shortest time required.
Which of the following is the release strategy you should use?

A. Red/Black deployment

B. Rolling deployment

C. ג€Big Bangג€ deployment

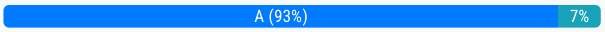
D. Canary deployment

Suggested Answer: *A*
Canary deployment -
With canary deployment, you deploy a new application code in a small part of the production infrastructure. Once the application is signed off for release, only a few users are routed to it. This minimizes any impact.
With no errors reported, the new version can gradually roll out to the rest of the infrastructure.
Reference:
https://dev.to/mostlyjason/intro-to-deployment-strategies-blue-green-canary-and-more-3a3

These days, the biggest change to software development is the frequency of deployments. Product teams deploy releases to production earlier (and more often). Months or years-long release cycles are becoming rare—especially among those building pure software products.

Today, using a service-oriented architecture and microservices approach, developers can design a code base to be modular. This allows them to write and deploy changes to different parts of the code base simultaneously.

Community vote distribution



waqas Highly Voted 2 years, 4 months ago
Selected Answer: A
A is the right anser. Blue/green and Red/Black are same. Must be 2 ['colored' paths] to swap immediately between them. Read the line "The strategy should also allow you to roll back in the shortest time required".So answer is A.
upvoted 32 times

UrbanRellik Most Recent 3 months ago
Selected Answer: A
A. Blue-Green deployment.
upvoted 2 times

UrbanRellik 3 months ago
This question appears much later in topic 7 or 8. The answer is "voted" to rolling deployment.

This question needs to be flagged for review or removal since there's contradicting information.
upvoted 2 times

UrbanRellik 2 months, 1 week ago
Statement withdrawn.
upvoted 2 times

vsvaid 8 months, 3 weeks ago
Selected Answer: A
I think A. Blue/Green deployment
upvoted 1 times

SolutionFinder 1 year ago
Cannot find Red/Black anywhere on MS pages. Maybe the term was changed in the past, meaning this question should be updated to current documentation and definitions. According to the current documentation only Canary release can be the correct one.
upvoted 4 times

Insanewhip 11 months ago
https://learn.microsoft.com/en-us/training/modules/implement-blue-green-deployment-feature-toggles/
upvoted 1 times

naivecoder786 1 year ago
Correct !`
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: A
Provided answer is correct
upvoted 2 times

Pavlo 1 year, 3 months ago
D. Canary deployment
upvoted 1 times

zellck 1 year, 3 months ago
Selected Answer: A
A is the answer.

https://learn.microsoft.com/en-us/training/modules/implement-blue-green-deployment-feature-toggles/2-what-blue-green-deployment
This technique can eliminate downtime because of app deployment. Besides, blue-green deployment reduces risk: if something unexpected happens with your new version on the green, you can immediately roll back to the last version by switching back to blue.
upvoted 4 times

mohiniu 1 year, 6 months ago
Canary should be right answer. As in case of red black deployment , application is deployed to black environment . Testing is done on black environment . Only after testing application is routed to black environment from red one. Canary can be faster but can have higher risk than red black
upvoted 1 times

Hieronimusov 1 year, 7 months ago
Selected Answer: A
Red/black = Blue/Green = 0X111/ 0X000
Its done with deployment slots which takes the time to minimum, and can be reversed at the same pace using swap operation.
upvoted 2 times

Hieronimusov 1 year, 7 months ago
0X111/ 0X000 that's a joke... ok? dont hate.
upvoted 2 times

reynaldo_aguiar 2 years ago
Answer section shows a description of Canary deployment instead of Blue/Green Deployment (Red/Black in this case) which is the right answer (A).
upvoted 4 times

syu31svc 2 years, 1 month ago
Selected Answer: A
Answer is A for sure
upvoted 2 times

Govcomm 2 years, 1 month ago
Red/Black with the deployment slots.
upvoted 2 times

Eltooth 2 years, 4 months ago
Selected Answer: A
A is correct answer however this is usually referred to as “Blue/Green”.
upvoted 4 times

UnknowMan 2 years, 4 months ago

Selected Answer: A

Correct (is like blue green)

upvoted 4 times

SlavMar 2 years, 4 months ago

It takes more time to run full deployment using Canary strategy.

Red/Black is more risky but faster.

Rollback from both might be same time

upvoted 3 times

Question #17 *Topic 1*

Your company hosts a web application in Azure, and makes use of Azure Pipelines for managing the build and release of the application.
When stakeholders report that system performance has been adversely affected by the most recent releases, you configure alerts in Azure Monitor.
You are informed that new releases must satisfy specified performance baseline conditions in the staging environment before they can be deployed to production.
You need to make sure that releases not satisfying the performance baseline are prevented from being deployed.
Which of the following actions should you take?

A. You should make use of a branch control check.

B. You should make use of an alert trigger.

C. You should make use of a gate.

D. You should make use of an approval check.

Suggested Answer: *C*
Scenarios and use cases for gates include:
➪ Quality validation. Query metrics from tests on the build artifacts such as pass rate or code coverage and deploy only if they are within required thresholds.
Use Quality Gates to integrate monitoring into your pre-deployment or post-deployment. This ensures that you are meeting the key health/performance metrics
(KPIs) as your applications move from dev to production and any differences in the infrastructure environment or scale is not negatively impacting your KPIs.
Note: Gates allow automatic collection of health signals from external services, and then promote the release when all the signals are successful at the same time or stop the deployment on timeout. Typically, gates are used in connection with incident management, problem management, change management, monitoring, and external approval systems.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/continuous-monitoring https://docs.microsoft.com/en-us/azure/devops/pipelines/release/approvals/gates?view=azure-devops

Community vote distribution

C (100%)

AlMargoi Highly Voted 2 years, 9 months ago
(Bill) Gates
upvoted 30 times

jojom19980 Highly Voted 3 years, 1 month ago
Correct, Gate
upvoted 13 times

yana_b Most Recent 1 year, 1 month ago
Selected Answer: C
Correct solution is to make use of gates
upvoted 1 times

yana_b 1 year, 1 month ago
Make use of gates as they allow allow automatic collection of health signals from external services and then promote the release when all the signals are successful or stop the deployment.
https://learn.microsoft.com/en-us/azure/devops/pipelines/release/approvals/gates?view=azure-devops
upvoted 3 times

Pavlo 1 year, 3 months ago
C. You should make use of a gate.
upvoted 1 times

zellck 1 year, 3 months ago
Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/devops/pipelines/release/approvals/gates?view=azure-devops
Gates allow automatic collection of health signals from external services and then promote the release when all the signals are successful or stop the deployment on timeout. Typically, gates are used in connection with incident management, problem management, change management, monitoring, and external approval systems.
upvoted 1 times

darko13 1 year, 7 months ago
"Releases prevented from being deployed" makes C correct, rather than D.
upvoted 1 times

PravinDhote 1 year, 8 months ago
Selected Answer: C
C - gate is correct ANS
upvoted 1 times

preethika1021 1 year, 9 months ago
Gate is correct
upvoted 2 times

GokhanSenyuz 1 year, 10 months ago
https://learn.microsoft.com/en-us/azure/devops/pipelines/release/approvals/?view=azure-devops
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: C
This is C for sure
upvoted 2 times

tjeerd 2 years, 1 month ago
Selected Answer: C
On exam 20220727.
upvoted 1 times

Govcomm 2 years, 1 month ago
Correct, use a gate.
upvoted 1 times

Dileep75 2 years, 2 months ago
We use gates for automated setup .. I think D is correct answer
upvoted 1 times

Dileep75 2 years, 2 months ago
ignore.. Gate is correct
upvoted 3 times

UnknowMan 2 years, 4 months ago
Selected Answer: C
Correct, with a gate you can query logs and metrics to take decision
upvoted 5 times

Eltooth 2 years, 4 months ago
Selected Answer: C
C is correct answer.
upvoted 2 times

rdemontis 2 years, 5 months ago
Selected Answer: C
correct answer
upvoted 2 times

Question #18 *Topic 1*

You need to consider the underlined segment to establish whether it is accurate.
To deploy an application to a number of Azure virtual machines, you should create a universal group.
Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required.

B. security

C. deployment

D. resource

Suggested Answer: *C*
When authoring an Azure Pipelines or TFS Release pipeline, you can specify the deployment targets for a job using a deployment group.
If the target machines are Azure VMs, you can quickly and easily prepare them by installing the Azure Pipelines Agent Azure VM extension on each of the VMs, or by using the Azure Resource Group Deployment task in your release pipeline to create a deployment group dynamically.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/release/deployment-groups

Azure Pipelines | Azure DevOps Server 2020 | Azure DevOps Server 2019 | TFS 2018

A deployment group is a logical set of deployment target machines that have agents installed on each one. Deployment groups represent the physical environments; for example, "Dev", "Test", or "Production" environment. In effect, a deployment group is just another grouping of agents, much like an agent pool.

Deployment groups are only available with Classic release pipelines and are different from deployment jobs. A deployment job is a collection of deployment-related steps defined in a YAML file to accomplish a specific task.

With deployment groups you can:

- Specify the security context and runtime targets for the agents. As you create a deployment group, you add users and give them appropriate permissions to administer, manage, view, and use the group.

Community vote distribution

C (100%)

syu31svc Highly Voted 2 years, 1 month ago
https://docs.microsoft.com/en-us/azure/devops/pipelines/release/deployment-groups/?view=azure-devops:

"A deployment group is a logical set of deployment target machines that have agents installed on each one. Deployment groups represent the physical environments; for example, "Dev", "Test", or "Production" environment. In effect, a deployment group is just another grouping of agents, much like an agent pool."

Answer is C
upvoted 11 times

4bd3116 Most Recent 4 months, 4 weeks ago
Selected Answer: C
A deployment group is a set of virtual machines with deployment agents. Every VM of the deployment group interacts with Azure Pipelines to coordinate the deployment tasks.
upvoted 1 times

jmglezgz 5 months ago
Selected Answer: C
Deployment groups

upvoted 1 times

yana_b 1 year, 1 month ago

Selected Answer: C

Correct answer is deployment group

upvoted 1 times

zellck 1 year, 3 months ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/devops/pipelines/release/deployment-groups/?view=azure-devops
A deployment group is a logical set of deployment target machines that have agents installed on each one. Deployment groups represent the physical environments; for example, "Dev", "Test", or "Production" environment. In effect, a deployment group is just another grouping of agents, much like an agent pool.

upvoted 3 times

PravinDhote 1 year, 8 months ago

Selected Answer: C

C - Deployment is correct ANS

upvoted 1 times

Matharax 1 year, 11 months ago

Selected Answer: C

Deployment groups is the correct answer

upvoted 4 times

Govcomm 2 years, 1 month ago

It should be deployment groups.

upvoted 1 times

Eltooth 2 years, 4 months ago

Selected Answer: C

C is correct answer - deployment group.

upvoted 3 times

Chiboy 2 years, 4 months ago

correct answer

upvoted 2 times

esend3 2 years, 4 months ago

Selected Answer: C

Deployment group

upvoted 3 times

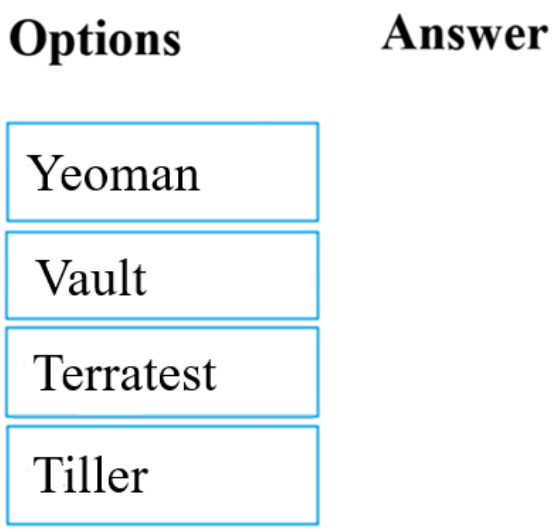
dupakonia 2 years, 4 months ago

correct

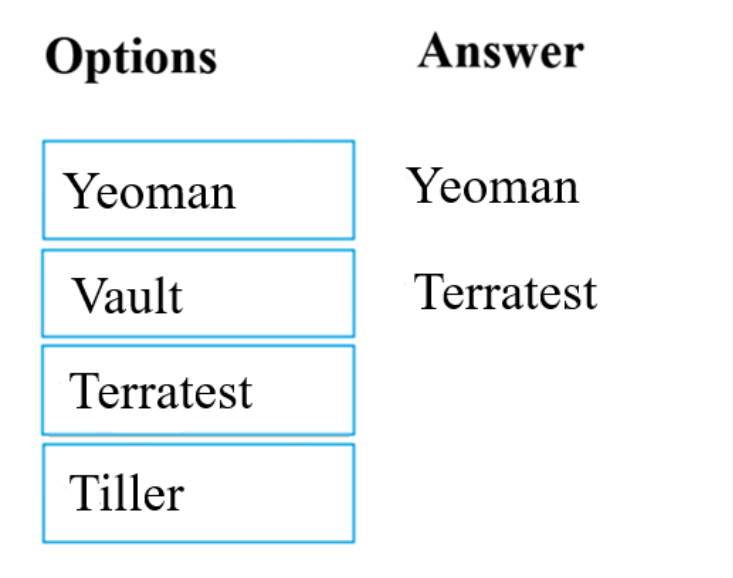
upvoted 2 times

Question #19 *Topic 1*

DRAG DROP -
You are preparing to deploy an Azure resource group via Terraform.
To achieve your goal, you have to install the necessary frameworks.
Which of the following are the frameworks you should use? Answer by dragging the correct options from the list to the answer area.
Select and Place:



Suggested Answer:



You can use the combination of Terraform and Yeoman. Terraform is a tool for creating infrastructure on Azure. Yeoman makes it easy to create Terraform modules.
Terratest provides a collection of helper functions and patterns for common infrastructure testing tasks, like making HTTP requests and using SSH to access a specific virtual machine. The following list describes some of the major advantages of using Terratest:
➪ Convenient helpers to check infrastructure - This feature is useful when you want to verify your real infrastructure in the real environment.
➪ Organized folder structure - Your test cases are organized clearly and follow the standard Terraform module folder structure.
Test cases are written in Go - Many developers who use Terraform are Go developers. If you're a Go developer, you don't have to learn another programming
▪ language to use Terratest.
➪ Extensible infrastructure - You can extend additional functions on top of Terratest, including Azure-specific features.
Reference:
https://docs.microsoft.com/en-us/azure/developer/terraform/create-base-template-using-yeoman https://docs.microsoft.com/en-us/azure/developer/terraform/test-modules-using-terratest

certstowinirl Highly Voted 2 years, 2 months ago

Very odd question... To reach the goal you don't need any of these frameworks. To deploy a resource group you would just need Terraform and the AzureRM provider
upvoted 39 times

syu31svc Highly Voted 2 years, 1 month ago
https://docs.microsoft.com/en-us/azure/developer/terraform/test-modules-using-terratest

Yeoman and Terratest are correct
upvoted 12 times

vsvaid Most Recent 9 months ago
Answer is correct. https://learn.microsoft.com/en-us/azure/developer/terraform/create-base-template-using-yeoman

Terraform is a tool for creating infrastructure on Azure. Yeoman makes it easy to create Terraform modules.
upvoted 1 times

yana_b 1 year, 1 month ago
IMHO it is Terratest and Yeoman
t's important to implement quality assurance when you create Terraform modules. We looked at all the most popular testing infrastructures and chose Terratest to use for testing our Terraform modules -> https://learn.microsoft.com/en-us/azure/developer/terraform/test-modules-using-terratest
Terraform is a tool for creating infrastructure on Azure. Yeoman makes it easy to create Terraform modules. -> https://learn.microsoft.com/en-us/azure/developer/terraform/create-base-template-using-yeoman

Tiller is Helms server-side component which runs inside the cluster and is used to deploy applications. The default installer of Tiller on an RBAC enabled cluster includes the creation of a service account for Tiller to run as which has cluster-admin permissions. ß: https://samcogan.com/tillerless-helm-with-azure-devops-pipelines/
upvoted 2 times

omerco61 1 year, 3 months ago
https://learn.microsoft.com/en-us/azure/developer/terraform/create-base-template-using-yeoman
upvoted 1 times

karrey 1 year, 4 months ago
Terratest
Vault
To deploy an Azure resource group via Terraform, you should use Terratest and Vault. Terratest is an open-source testing framework for testing infrastructure code, such as Terraform scripts, which helps you ensure that your infrastructure is correctly provisioned. Vault is a tool for managing secrets, such as API keys and credentials, that are needed during the deployment process. Using these two frameworks together will help you securely deploy and manage your Azure resource group using Terraform.

#ChatGPT-4
upvoted 1 times

col2511kol 1 year, 5 months ago
To deploy an Azure resource group via Terraform, you will need Terraform. This is the primary tool for defining, provisioning, and managing infrastructure as code. It supports multiple cloud providers, including Azure.
None of the options provided are required to deploy an Azure resource group via Terraform.
upvoted 3 times

Fal991l 1 year, 5 months ago
None of the options provided in the selected text are necessary frameworks for deploying an Azure resource group via Terraform. To deploy an Azure resource group using Terraform, you need to have Terraform installed and configured 1. You also need to have an Azure subscription 1. Once you have these prerequisites, you can create Terraform configuration files using HCL syntax to specify the cloud provider (such as Azure) and the elements that make up your cloud infrastructure 1.
upvoted 2 times

omsingh 1 year, 6 months ago
yeoman, vault and terratest will be correct answer
upvoted 1 times

JeevanKumar 2 years, 1 month ago

Agree. Deployment doesn't require both of the framework. It just require Terraform and AzureRM provider blocks. They should elaborate requirement for both of the framework.

upvoted 4 times

Divyayuvi 2 years, 3 months ago

answer is correct.

upvoted 1 times

Anirbanfiem 2 years, 3 months ago

what will be the correct answer ?

upvoted 1 times

Lucario95 2 years, 4 months ago

I'll say Vault and Terratest just because they're HashiiCorp software...

upvoted 1 times

Training 2 years, 4 months ago

Terratest is not from Hashicorp. Vault is a different product than IAC. Its secrets mgmt solution from Hashicorp.

upvoted 3 times

Question #20 *Topic 1*

You intend to make use of Azure Artifacts to share packages that you wrote, tested, validated, and deployed.
You want to use a solitary feed to release several builds of each package. You have to make sure that the release of packages that are in development is restricted.
Which of the following actions should you take?

A. You should make use of static code analysis.

B. You should make use of views.

C. You should make use of dynamic code analysis.

D. You should make use of upstream sources.

Suggested Answer: *D*
Upstream sources enable you to manage all of your product's dependencies in a single feed. We recommend publishing all of the packages for a given product to that product's feed, and managing that product's dependencies from remote feeds in the same feed, via upstream sources. This setup has a few benefits:
➪ Simplicity: your NuGet.config, .npmrc, or settings.xml contains exactly one feed (your feed).
➪ Determinism: your feed resolves package requests in order, so rebuilding the same codebase at the same commit or changeset uses the same set of packages
➪ Provenance: your feed knows the provenance of packages it saved via upstream sources, so you can verify that you're using the original package, not a custom or malicious copy published to your feed
➪ Peace of mind: packages used via upstream sources are guaranteed to be saved in the feed on first use; if the upstream source is disabled/removed, or the remote feed goes down or deletes a package you depend on, you can continue to develop and build
Reference:
https://docs.microsoft.com/en-us/azure/devops/artifacts/concepts/upstream-sources?view=vsts

Community vote distribution

megaejay Highly Voted 3 years, 2 months ago
correct Answer is B
upvoted 37 times

kiko90909 1 month, 1 week ago
To ensure that the release of packages in development is restricted while using a solitary feed in Azure Artifacts, you should make use of views (Option B). Views in Azure Artifacts allow you to filter and control the visibility of packages
upvoted 1 times

kanompia 3 years, 2 months ago
Agree with B, a view feed
upvoted 6 times

ThomasKong Highly Voted 3 years, 1 month ago
Based on the link https://docs.microsoft.com/en-us/azure/devops/artifacts/concepts/views?view=azure-devops,

use of feed - "is to share package versions that have been tested and validated but hold back on packages that are still under development and/or didn't meet your quality bar."

for Upsteam sources - "In order for other Azure Artifacts feeds to use your feed as an upstream source, you must set your feed's view visibility to members of your organization, or members of your Azure Active Directory, depending on your scenario."

I think, since it deployment phase/stage, the view should be start first after that only upstream sources to control who I would like to share.

I will go with - B.
upvoted 26 times

sondrex Most Recent 1 month, 3 weeks ago
must be D

upvoted 1 times

sondrex 1 month, 3 weeks ago

not correct

Using views in Azure Artifacts allows you to manage and restrict access to specific versions of packages. Views let you create stages (such as @local, @prerelease, and @release) that control which versions of the packages are visible and accessible to different users. This ensures that only stable and tested versions are promoted to the production view, keeping development versions restricted.

Upstream sources are used to connect to external package sources but don't inherently provide the same level of control for restricting access to development packages.

Correct action: B. You should make use of views.

upvoted 1 times

FeriAZ 6 months, 2 weeks ago

Selected Answer: B

Views allow you to create a filtered version of a feed, showing only specific packages or versions that meet your criteria. You can create a view that excludes packages marked as "development" from being accessed by users, even though they exist in the original feed.

upvoted 3 times

vsvaid 8 months, 3 weeks ago

Selected Answer: B

I think views

upvoted 1 times

yana_b 1 year, 1 month ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/devops/artifacts/concepts/views?view=azure-devops -> A common use of feed views is to share package versions that have been tested and validated but hold back on packages that are still under development ...

upvoted 4 times

Msds1981 1 year, 1 month ago

Selected Answer: B

Answer is B. Explanation:

In Azure Artifacts, views allow you to control access to packages within a feed. By creating views, you can define specific rules and filters to restrict the visibility of packages based on certain criteria. This includes restricting access to packages that are still in development.

upvoted 2 times

itexamsmicrosoft 1 year, 2 months ago

Selected Answer: B

B. You should make use of views.

B. You should make use of views: Views in Azure Artifacts help you manage and consume packages in your feed. By default, each feed in Azure Artifacts has three views: @local, @Prerelease, and @Release. You can promote a package version from one view to another to control its visibility and availability. This can help you to restrict the release of packages that are still in development.

In Azure Artifacts, Views are a feature designed to help manage the release and visibility of packages in your feed, making them the most suitable choice for this scenario.

upvoted 6 times

elmarkos23 1 year, 2 months ago

Selected Answer: B

B. You should make use of views.

Views in Azure Artifacts allow you to control the visibility and access to specific packages within a feed. By creating views, you can restrict the release of packages that are still in development and control who has access to them.

You can configure views to include or exclude specific packages based on criteria such as version ranges, tags, or other metadata. This allows you to define separate views for different stages of development, such as a "Development" view for packages still in progress and a "Release" view for packages that have been validated and are ready for deployment.

By using views, you can effectively restrict the release of packages that are in development while using a single feed in Azure Artifacts. This helps maintain control over the availability and visibility of packages to different teams and stakeholders.

Options A, C, and D are not the most appropriate actions
upvoted 2 times

Pavlo 1 year, 3 months ago
BBBBBBBBBBBBBBBBB (B)
upvoted 2 times

zellck 1 year, 3 months ago
Selected Answer: B
B is the answer.

https://learn.microsoft.com/en-us/azure/devops/artifacts/concepts/views?view=azure-devops
Feed views enable developers to share a subset of package-versions with their consumers. A common use of feed views is to share package versions that have been tested and validated but hold back on packages that are still under development and/or didn't meet a certain quality bar.
upvoted 3 times

Pukun 1 year, 3 months ago
correct Answer is B

Views in Azure Artifacts allow you to control access to specific packages within a feed. You can create views to include or exclude packages based on specific criteria, such as package version, tags, or other metadata. By configuring views, you can restrict the release of packages that are still in development to only authorized users or groups.
upvoted 1 times

omsingh 1 year, 6 months ago
B. You should make use of views.

To restrict the release of packages that are in development, you should use views in Azure Artifacts. Views are a way to manage the visibility of packages in a feed. You can create views that are specific to certain groups or teams in your organization, and control which packages are visible to those groups.

By creating a view for packages that are ready for release, you can restrict the visibility of packages that are still in development. Only the packages in the view will be available for use, while the packages that are still in development will remain hidden.

Static code analysis and dynamic code analysis are techniques for analyzing code to find errors or vulnerabilities, and are not directly related to managing package visibility in Azure Artifacts. Upstream sources are used to pull packages from external sources into your feed, and are not related to managing package visibility within your feed. Therefore, options A, C, and D are not relevant for this scenario.
upvoted 2 times

srine69 1 year, 12 months ago
Selected Answer: B
Why doesn't someone fix this? It is clearly B.
upvoted 3 times

Tranquillo1811 2 years ago
I'm not quite sure, whether B is correct, because while views allow to filter the packages of a feed, the packages can still be accessed (and released) from the @local view...?
upvoted 2 times

syu31svc 2 years, 1 month ago
Selected Answer: B
What are feed views?

Feed views enable developers to share a subset of package-versions with their consumers. A common use of feed views is to share package versions that have been tested and validated but hold back on packages that are still under development and/or didn't meet a certain quality bar.

From https://docs.microsoft.com/en-us/azure/devops/artifacts/concepts/views?view=azure-devops

Answer is B
upvoted 5 times

Tranquillo1811 2 years ago

ok, forget about my comment. Just read about upstream sources and since they do NOT allow package restriction, feed views are the only valid option...

upvoted 2 times

tjeerd 2 years, 1 month ago

Selected Answer: B

On exam 20220727.

upvoted 4 times

Question #21 *Topic 1*

You need to consider the underlined segment to establish whether it is accurate.
To find when common open source libraries are added to the code base, you should add Jenkins to the build pipeline.
Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required.

B. SourceGear Vault

C. WhiteSource

D. OWASP ZAP

Suggested Answer: *C*
WhiteSource is the leader in continuous open source software security and compliance management. WhiteSource integrates into your build process, irrespective of your programming languages, build tools, or development environments. It works automatically, continuously, and silently in the background, checking the security, licensing, and quality of your open source components against WhiteSource constantly-updated definitive database of open source repositories.
Azure DevOps integration with WhiteSource Bolt will enable you to:
1. Detect and remedy vulnerable open source components.
2. Generate comprehensive open source inventory reports per project or build.
3. Enforce open source license compliance, including dependencies' licenses.
4. Identify outdated open source libraries with recommendations to update.
Note: Black duck would also be a good answer, but it is not an option here.
Reference:
https://www.azuredevopslabs.com/labs/vstsextend/WhiteSource/

Community vote distribution
C (100%)

tinox63144 Highly Voted 1 year, 10 months ago
WhiteSource is now called Mend.
upvoted 18 times

FeriAZ Most Recent 5 months, 4 weeks ago
Selected Answer: C
WhiteSource, is a code security analysis tool capable of identifying open-source libraries within your codebase. Additionally, some WhiteSource features track changes over time, potentially allowing you to pinpoint when specific libraries were introduced.
upvoted 1 times

kleansoul 12 months ago
Selected Answer: C
WhiteSource also known as MEND is used for open source code security. Therefore it is the right answer to be added to build pipeline.
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: C
Correct answer is WhiteSource
upvoted 1 times

Msds1981 1 year, 1 month ago
Selected Answer: C
answer is C .
WhiteSource is a tool commonly used for open source component management and security. It helps organizations identify and track open source libraries and dependencies used in their codebase. By integrating WhiteSource into the build pipeline, you can automatically detect and monitor the inclusion of open source libraries, check for security vulnerabilities, and ensure compliance with licenses.
upvoted 2 times

zellck 1 year, 3 months ago
Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/visualstudio/subscriptions/vs-whitesource
upvoted 3 times

zellck 1 year, 3 months ago
https://marketplace.visualstudio.com/items?itemName=whitesource.whitesource
WhiteSource integrates with your CI servers, build tools and repositories to detect all open source components in your software, without ever scanning your code. It provides you with real-time alerts on vulnerable or problematic components, generates comprehensive up-to-date reports in one-click and enables you to streamline your entire open source management process with automated policies.
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: C
This is C for sure
upvoted 1 times

Govcomm 2 years, 1 month ago
Open source libraries using WhiteSources.
upvoted 1 times

Eltooth 2 years, 3 months ago
Selected Answer: C
C is correct answer.
upvoted 1 times

UnknowMan 2 years, 4 months ago
Selected Answer: C
Correct
upvoted 2 times

rdemontis 2 years, 5 months ago
Selected Answer: C
answer is correct. you can also use Black Duck
upvoted 3 times

AlMargoi 2 years, 9 months ago
Whitsource
upvoted 3 times

jojom19980 3 years, 1 month ago
yes, WhiteSource
upvoted 4 times

Question #22 *Topic 1*

Your company has an Azure DevOps project, which includes a build pipeline that makes use of roughly fifty open source libraries.
You have been tasked with making sure that you are able to scan project for common security weaknesses in the open source libraries.
Which of the following actions should you take?

A. You should create a build task and use the WhiteSource Bolt service.

B. You should create a deployment task and use the WhiteSource Bolt service.

C. You should create a build task and use the Chef service.

D. You should create a deployment task and use the Chef service.

Suggested Answer: *A*
Reference:
https://www.azuredevopslabs.com/labs/vstsextend/whitesource/

Community vote distribution
A (100%)

jojom19980 Highly Voted 3 years, 1 month ago
yes , in build stage
upvoted 8 times

hikhatri Highly Voted 3 years, 2 months ago
The given answer is correct
upvoted 6 times

FeriAZ Most Recent 6 months, 2 weeks ago
Selected Answer: A
Since you need to scan your codebase during the build process to identify vulnerabilities in open-source libraries, the most suitable option is:

A. You should create a build task and use the WhiteSource Bolt service.

This approach leverages the build task within your Azure DevOps pipeline, ensuring the scan happens early in the development lifecycle, allowing you to address potential vulnerabilities before deployment.
WhiteSource Bolt is a specific solution designed to address your exact requirement of scanning open-source libraries for vulnerabilities.
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: A
Create a build task and use the WhiteSource Bolt service.
upvoted 1 times

zellck 1 year, 3 months ago
Selected Answer: A
A is the answer.

https://learn.microsoft.com/en-us/visualstudio/subscriptions/vs-whitesource
upvoted 3 times

zellck 1 year, 3 months ago
https://marketplace.visualstudio.com/items?itemName=whitesource.whitesource
WhiteSource integrates with your CI servers, build tools and repositories to detect all open source components in your software, without ever scanning your code. It provides you with real-time alerts on vulnerable or problematic components, generates comprehensive up-to-date reports in one-click and enables you to streamline your entire open source management process with automated policies.
upvoted 1 times

zellck 1 year, 3 months ago

A is the answer.

https://learn.microsoft.com/en-us/visualstudio/subscriptions/vs-whitesource
upvoted 1 times

nasmieci 1 year, 11 months ago

Selected Answer: A

A is correct answer
upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: A

C and D are out for sure

Between A and B, A is correct

Build task not deployment
upvoted 2 times

Govcomm 2 years, 1 month ago

Build task with WhilteSource Bolt
upvoted 1 times

Eltooth 2 years, 3 months ago

Selected Answer: A

A is correct answer.
upvoted 2 times

UnknowMan 2 years, 4 months ago

Selected Answer: A

Correct
upvoted 1 times

Mcelona 2 years, 4 months ago

Selected Answer: A

correct
upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: A

correct, whitesource is the tool and it should be used on CI phase.
upvoted 2 times

Question #23 *Topic 1*

You need to consider the underlined segment to establish whether it is accurate.
Black Duck can be used to make sure that all the open source libraries conform to your company's licensing criteria.
Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required.

B. Maven

C. Bamboo

D. CMAKE

Suggested Answer: *A*
Secure and Manage Open Source Software
Black Duck helps organizations identify and mitigate open source security, license compliance and code-quality risks across application and container portfolios.
Black Duck Hub and its plugin for Team Foundation Server (TFS) allows you to automatically find and fix open source security vulnerabilities during the build process, so you can proactively manage risk. The integration allows you to receive alerts and fail builds when any Black Duck Hub policy violations are met.
Reference:
https://marketplace.visualstudio.com/items?itemName=black-duck-software.hub-tfs

Community vote distribution

yana_b 1 year, 1 month ago

Selected Answer: A

Correct answer is A

upvoted 1 times

Msds1981 1 year, 1 month ago

Selected Answer: A

Black Duck is a popular tool used for open source security and license compliance management. It can be used to ensure that all the open source libraries used in a project conform to your company's licensing criteria. Black Duck scans the codebase, identifies the open source components, and checks their licenses against a predefined set of policies to ensure compliance with legal and company-specific licensing requirements.

upvoted 3 times

zellck 1 year, 3 months ago

Selected Answer: A

A is the answer.

https://marketplace.visualstudio.com/items?itemName=black-duck-software.detect-for-tfs
The Black Duck by Synopsys plugin for TFS and Azure DevOps allows automatic identification of open source security vulnerabilities during your application build process. The integration allows you to enforce policies configured in Black Duck to receive alerts and fail builds when policy violations are met.

upvoted 4 times

syu31svc 2 years, 1 month ago

Selected Answer: A

Answer is A for sure

upvoted 2 times

kennynelcon 2 years, 1 month ago

Selected Answer: A

Since BlackDuck is accurate, No adjustments needed

upvoted 2 times

Govcomm 2 years, 1 month ago

BlackDuck or WhilteSource.

upvoted 3 times

Eltooth 2 years, 3 months ago

Selected Answer: A

A is correct answer.

upvoted 1 times

Chiboy 2 years, 4 months ago

correct

upvoted 1 times

UnknowMan 2 years, 4 months ago

Selected Answer: A

Correct

upvoted 1 times

Mcelona 2 years, 4 months ago

Selected Answer: A

correct

upvoted 2 times

dupakonia 2 years, 4 months ago

correct

upvoted 2 times

Question #24 *Topic 1*

You have created an Azure DevOps project for a new application that will be deployed to a number of Windows Server 2016 Azure virtual machines.
You are preparing a deployment solution that allows for the virtual machines to maintain a uniform configuration, and also keep administrative effort with regards to configuring the virtual machines to a minimum.
Which of the following should be part of your solution? (Choose two.)

A. Azure Resource Manager templates

B. The PowerShell Desired State Configuration (DSC) extension for Windows

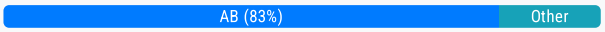
C. Azure pipeline deployment groups

D. The Custom Script Extension for Windows

E. Azure pipeline stage templates

Suggested Answer: *AD*
The Custom Script Extension downloads and executes scripts on Azure virtual machines. This extension is useful for post deployment configuration, software installation, or any other configuration or management tasks. Scripts can be downloaded from Azure storage or GitHub, or provided to the Azure portal at extension run time. The Custom Script Extension integrates with Azure Resource Manager templates, and can be run using the Azure CLI, PowerShell, Azure portal, or the Azure Virtual Machine REST API.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/custom-script-windows

Community vote distribution



balajim212 Highly Voted 3 years, 2 months ago
Correct answer is A & B
upvoted 35 times

rdemontis Highly Voted 2 years, 5 months ago
Selected Answer: AB
Considering the requirements
- maintain a uniform configuration for virtual machines
- minimize administrative effort

I think correct answer is A & B.
To mantain the configuration status of a VM you must use DSC.
To minimize the effort of creating the VM you can use an ARM template so that you can reuse it for each VM. Deployment groups requires more effort.

https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-template
https://docs.microsoft.com/en-us/azure/devops/pipelines/release/deployment-groups/?view=azure-devops
upvoted 23 times

deltarj 2 years, 3 months ago
Yap, I agree.. seems "maintain" is the key word.
upvoted 7 times

OlehT Most Recent 2 months ago
Selected Answer: AB
The Azure DSC extension uses the Azure VM Extension framework to deliver, enact, and report on DSC configurations running on Azure VMs.

The most common approach for deploying the DSC extension is to use Azure Resource Manager templates.

https://learn.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview
upvoted 1 times

FeriAZ 6 months, 2 weeks ago

Selected Answer: AB

A. Azure Resource Manager (ARM) templates: These are JSON files that define the infrastructure and configuration of your Azure resources, including virtual machines. Using ARM templates ensures consistent configuration across all VMs by defining the desired state in code. This facilitates repeatable and automated deployments, reducing manual configuration and potential errors.

B. PowerShell Desired State Configuration (DSC) extension for Windows: This extension allows you to manage the configuration of your Windows VMs using DSC in an automated fashion. DSC leverages declarative scripts to specify the desired state of the system, and the extension ensures that the VMs converge towards that configuration state. This method simplifies management and reduces administrative effort, as you can configure settings centrally through DSC scripts rather than manually on each VM.

upvoted 1 times

vsvaid 9 months ago

Correct answer is A&B

upvoted 1 times

vsvaid 9 months ago

Selected Answer: B

Power DSC extension will be installed on node when connected to Azure Automation. B is correct answer

upvoted 1 times

vsvaid 8 months, 3 weeks ago

Ignore my previous answer, please select AB

upvoted 1 times

kleansoul 12 months ago

Selected Answer: AD

A & C is the correct answer.

DSC will keep the desired state of the config but here the question states that the minimum effort required from Azure DevOps which is done using Deployment Scripts which is custom scripts extension for Windows.

upvoted 3 times

ieboaix 1 year, 1 month ago

agree with A & B

upvoted 1 times

yana_b 1 year, 1 month ago

Selected Answer: AB

https://learn.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-windows

The PowerShell DSC Extension for Windows is published and supported by Microsoft. The extension uploads and applies a PowerShell DSC Configuration on an Azure VM. The DSC Extension calls into PowerShell DSC to enact the received DSC configuration on the VM.

Azure VM extensions can be deployed with Azure Resource Manager templates. Templates are ideal when deploying one or more virtual machines that require post deployment configuration.

A newer version of DSC is now generally available, managed by a feature of Azure Automange named machine configuration. The machine configuration feature combines features of the Desired State Configuration (DSC) extension handler, Azure Automation State Configuration, and the most commonly requested features from customer feedback.

upvoted 1 times

Msds1981 1 year, 1 month ago

Selected Answer: AB

A. Azure Resource Manager templates: Azure Resource Manager (ARM) templates are declarative templates that define the infrastructure and configuration of your Azure resources. With ARM templates, you can define the virtual machines' configuration, including their operating system, networking, storage, and more. By using ARM templates, you can ensure that all virtual machines are deployed with a consistent and standardized configuration, reducing manual effort and minimizing configuration drift.

B. The PowerShell Desired State Configuration (DSC) extension for Windows: DSC is a feature in PowerShell that enables you to declare and manage the configuration of target nodes, such as Windows Server 2016 virtual machines. By using the DSC extension in Azure DevOps, you can apply and enforce the desired configuration on the virtual machines during the deployment process. DSC ensures that the virtual machines remain in the desired state, and any configuration drift is automatically corrected.

upvoted 4 times

Pavlo 1 year, 3 months ago

A & B <_____>

upvoted 2 times

Procurement 1 year, 3 months ago

Selected Answer: AB

Correct answer is A & B

upvoted 3 times

zellck 1 year, 3 months ago

Selected Answer: AB

AB is the answer.

https://learn.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview
The primary use for the Azure Desired State Configuration (DSC) extension for Windows PowerShell is to bootstrap a VM to the Azure Automation State Configuration (DSC) service. This service provides benefits that include ongoing management of the VM configuration and integration with other operational tools, such as Azure Monitor. You can use the extension to register your VMs to the service and gain a flexible solution that works across Azure subscriptions.

upvoted 3 times

MrKingpin 1 year, 6 months ago

Similar question where A&B vs. A&D are combined into a single answer
https://www.examtopics.com/discussions/microsoft/view/16114-exam-az-400-topic-6-question-12-discussion/

upvoted 1 times

jojorabbit2021 1 year, 7 months ago

Selected Answer: AB

A & B correct

upvoted 3 times

Whatsamattr81 1 year, 7 months ago

Changing my last answer... "keep administrative effort with regards to configuring the virtual machines to a minimum" - that's definitely NOT DSC. ARM and Extensions.

upvoted 1 times

Whatsamattr81 1 year, 7 months ago

Maintain a uniform configuration with minimal administrative effort... the answers is clearly DSC.. and if you were using DSC, you wouldn't need to use a custom script extension. So logically (IMHO) it can only be ARM and DSC

upvoted 1 times

Question #25 *Topic 1*

Your company has an application that contains a number of Azure App Service web apps and Azure functions.
You would like to view recommendations with regards to the security of the web apps and functions. You plan to navigate to Compute and Apps to achieve your goal.
Which of the following should you access to make use of Compute and Apps?

A. Azure Log Analytics

B. Azure Event Hubs

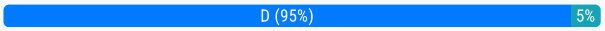
C. Azure Advisor

D. Azure Security Center

Suggested Answer: *D*
Monitor compute and app services: Compute & apps include the App Services tab, which App services: list of your App service environments and current security state of each.

Recommendations -
This section has a set of recommendations for each VM and computer, web and worker roles, Azure App Service Web Apps, and Azure App Service Environment that Security Center monitors. The first column lists the recommendation. The second column shows the total number of resources that are affected by that recommendation. The third column shows the severity of the issue.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/proactive-diagnostics

Community vote distribution



simoziyadi Highly Voted 2 years, 9 months ago
Azure Security Center and Azure Defender are now called Microsoft Defender for Cloud.
upvoted 32 times

joancar2009 Highly Voted 3 years, 2 months ago
Correct
upvoted 9 times

alirezak22 Most Recent 2 months, 1 week ago
Selected Answer: D
d i correct, since it uses microsoft defender
upvoted 1 times

OlehT 2 months, 1 week ago
Selected Answer: C
I think this question in old now and will/or already updated.
You can go to security from Advisor, second there is no Azure Security Center, now it is Security.
Also, question asks about recommendations and recommendations are only in Advisor --> Security.
upvoted 1 times

AppleVan 1 year ago
Why not C? Azure advisor also recommends about security..
upvoted 7 times

alirezak22 2 months, 1 week ago
D is correct, since it uses MS Defender,
upvoted 1 times

OlehT 2 months, 1 week ago
Good point, this was my answer. I think this question in old now and will/or already updated.
You can go to security from Advisor, second there is no Azure Security Center, now it is Security.
Also, question asks about recommendations and recommendations are only in Advisor --> Security.
upvoted 1 times

yana_b 1 year, 1 month ago

Selected Answer: D

Provided answer is correct

upvoted 1 times

Hieronimusov 1 year, 7 months ago

Selected Answer: D

D - Microsoft Defender for Cloud

upvoted 6 times

Jawad1462 1 year, 10 months ago

Selected Answer: D

Given answer is correct

upvoted 2 times

syu31svc 2 years, 1 month ago

Selected Answer: D

"recommendations with regards to the security"

Answer is D (now called Microsoft Defender for Cloud)

upvoted 4 times

Govcomm 2 years, 1 month ago

Defender for the Cloud

upvoted 1 times

Eltooth 2 years, 3 months ago

Selected Answer: D

D is correct answer.

upvoted 1 times

UnknowMan 2 years, 4 months ago

Selected Answer: D

Correct

upvoted 1 times

Mcelona 2 years, 4 months ago

Selected Answer: D

Correct

upvoted 1 times

vvkds 2 years, 5 months ago

Now it's Microsoft Defender for Cloud

upvoted 5 times

rdemontis 2 years, 5 months ago

Selected Answer: D

correct answer

upvoted 2 times

Kazillius 3 years, 2 months ago

Correct answer.

upvoted 3 times

Question #26 *Topic 1*

You need to consider the underlined segment to establish whether it is accurate.
Your company has a multi-tier application that has its front end hosted in Azure App Service.
To pinpoint the average load times of the application pages, you should make use of Azure Event Hubs.
Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required.

B. Azure Application Insights

C. Azure Log Analytics

D. Azure Advisor

Suggested Answer: *B*
Application Insights will tell you about any performance issues and exceptions, and help you find and diagnose the root causes.
Application Insights can monitor both Java and ASP.NET web applications and services, WCF services. They can be hosted on-premises, on virtual machines, or as Microsoft Azure websites.
On the client side, Application Insights can take telemetry from web pages and a wide variety of devices including iOS, Android, and Windows Store apps.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/web-monitor-performance

Community vote distribution
B (100%)

Ash111 Highly Voted 3 years, 2 months ago
Given answer is correct
upvoted 17 times

FeriAZ Most Recent 6 months, 2 weeks ago
Selected Answer: B
Application Insights

Monitors web applications and services: Collects performance-related data, including page load times, user engagement, and exceptions.
Provides detailed insights: Analyzes data to identify performance bottlenecks and application health issues.
Offers visualizations: Presents data in dashboards and reports for easy understanding.
upvoted 1 times

gabo 11 months, 3 weeks ago
Multi tier application = Web Application, so Application Insights makes more sense.
upvoted 2 times

yana_b 1 year, 1 month ago
Selected Answer: B
Correct answer is B
upvoted 1 times

Msds1981 1 year, 1 month ago
Selected Answer: B
Azure Application Insights is a powerful monitoring and application performance management (APM) service in Azure. It is specifically designed to provide insights into the performance and usage of web applications, including front-end hosted in Azure App Service.
upvoted 2 times

zellck 1 year, 3 months ago
Selected Answer: B
B is the answer.

https://learn.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview?tabs=net
Application Insights is an extension of Azure Monitor and provides application performance monitoring (APM) features. APM tools are useful to monitor applications from development, through test, and into production in the following ways:

- Proactively understand how an application is performing.
- Reactively review application execution data to determine the cause of an incident.

upvoted 3 times

syu31svc 2 years, 1 month ago

Selected Answer: B

This is B for sure

upvoted 2 times

Govcomm 2 years, 1 month ago

Azure application insights for the load time.

upvoted 1 times

Eltooth 2 years, 3 months ago

Selected Answer: B

B is correct answer.

upvoted 1 times

UnknowMan 2 years, 4 months ago

Selected Answer: B

Correct

upvoted 2 times

Mcelona 2 years, 4 months ago

Selected Answer: B

Correct

upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: B

correct

https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview

upvoted 2 times

gOKU 2 years, 8 months ago

correct

upvoted 2 times

Question #27 *Topic 1*

Your company makes use of Azure SQL Database Intelligent Insights and Azure Application Insights for monitoring purposes.
You have been tasked with analyzing the monitoring using ad-hoc queries. You need to utilize the correct query language.
Solution: You use the Contextual Query Language (CQL).
Does the solution meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/insights/azure-sql

Community vote distribution

B (100%)

saschgo Highly Voted 3 years, 2 months ago
Answer B. No

Presumably "Kusto Query Language (KQL)" would be the right answer.
upvoted 20 times

FeriAZ Most Recent 6 months, 2 weeks ago
Selected Answer: B
Azure SQL Database Intelligent Insights and Azure Application Insights use Kusto Query Language (KQL) for ad-hoc queries.
CQL is primarily used for querying Azure Monitor logs.
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: B
Should be yes when provided solution of this question is KQL (Kusto query language)
upvoted 1 times

zellck 1 year, 3 months ago
Selected Answer: B
B is the answer.

https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-query-overview
Azure Monitor Logs is based on Azure Data Explorer, and log queries are written by using the same Kusto Query Language (KQL). This rich language is designed to be easy to read and author, so you should be able to start writing queries with some basic guidance.
upvoted 3 times

ShomaV 1 year, 3 months ago
Azure Application Insights, you would use the Application Insights Analytics query language. This query language is based on a subset of the Kusto Query Language (KQL) and allows you to perform advanced analytics and querying on your application telemetry data.
upvoted 1 times

Matharax 1 year, 11 months ago
Selected Answer: B
Answer is 'No'. Should be KQL.
upvoted 2 times

syu31svc 2 years, 1 month ago
Selected Answer: B
Answer is No; it's KQL
upvoted 1 times

hellovanduc 2 years, 1 month ago
The reference link should be: https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-query-overview
upvoted 2 times

Govcomm 2 years, 1 month ago

No, KQL

upvoted 1 times

Eltooth 2 years, 3 months ago

Selected Answer: B

B is correct answer.

KQL needed.

upvoted 2 times

UnknowMan 2 years, 4 months ago

Correct => Use KQL (Kusto)

upvoted 2 times

Mcelona 2 years, 4 months ago

Selected Answer: B

Right answer is No.

upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: B

both services (Azure SQL Database Intelligent Insights and Application Insights) could send data to Azure Monitor Logs so you can use KQL to do queries.

upvoted 2 times

Aniruddha_dravyakar 2 years, 11 months ago

KQL is the right answer

upvoted 1 times

Question #28 *Topic 1*

Your company makes use of Azure SQL Database Intelligent Insights and Azure Application Insights for monitoring purposes.
You have been tasked with analyzing the monitoring using ad-hoc queries. You need to utilize the correct query language.
Solution: You use the Transact-SQL.
Does the solution meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/insights/azure-sql

Community vote distribution

B (100%)

lesiris Highly Voted 3 years, 2 months ago
I guess the right answer is Kusto Language
upvoted 11 times

mahiAzure20 Most Recent 3 months ago
Transact-SQL (T-SQL) for Azure SQL Database Intelligent Insights.
Kusto Query Language (KQL) for Azure Application Insights.
Answer is Yes
upvoted 1 times

FeriAZ 6 months, 2 weeks ago
Azure SQL Database Intelligent Insights and Azure Application Insights use Kusto Query Language (KQL) for ad-hoc queries.
CQL is primarily used for querying Azure Monitor logs.
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: B
Solution for this is KQL (Kusto query language)
upvoted 1 times

zellck 1 year, 3 months ago
Selected Answer: B
B is the answer.

https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-query-overview
Azure Monitor Logs is based on Azure Data Explorer, and log queries are written by using the same Kusto Query Language (KQL). This rich language is designed to be easy to read and author, so you should be able to start writing queries with some basic guidance.
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: B
Answer is No; KQL instead
upvoted 2 times

Govcomm 2 years, 1 month ago
No, KQL
upvoted 2 times

Eltooth 2 years, 3 months ago
Selected Answer: B
B is correct answer.
KQL is needed.
upvoted 2 times

UnknowMan 2 years, 4 months ago

Selected Answer: B

Correct

upvoted 1 times

Mcelona 2 years, 4 months ago

Selected Answer: B

No is the right answer.

upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: B

correct answer. KQL is the language to use in this case

upvoted 1 times

Sara_Mo 2 years, 7 months ago

No. its Kusto Language (KQL)

upvoted 1 times

ScreamingHand 3 years, 1 month ago

To work with Log Analytics data, you need to use the Kusto Query Language (KQL)

upvoted 4 times

Question #29 *Topic 1*

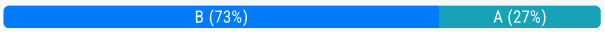
Your company makes use of Azure SQL Database Intelligent Insights and Azure Application Insights for monitoring purposes.
You have been tasked with analyzing the monitoring using ad-hoc queries. You need to utilize the correct query language.
Solution: You use Azure Log Analytics.
Does the solution meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Data analysis in Azure SQL Analytics is based on Log Analytics language for your custom querying and reporting.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/insights/azure-sql

Community vote distribution



fanq10 Highly Voted 3 years, 2 months ago
You need to utilize the correct query language.
Azure Log Analytics is NOT a query language. So Given answer is correct
upvoted 50 times

AzureJobsTillRetire 1 year, 8 months ago
This is not correct. The question does not specifically ask which language you should use. It states that you need to utilize the correct query language, and you can do so by using Azure Log Analytics, which has KQL inside you can use.
upvoted 11 times

marras 2 years, 3 months ago
I'd prefer KQL however Microsoft calls Log Analytics also a language here: https://docs.microsoft.com/en-us/services-hub/health/log_analytics_query_language
upvoted 6 times

pdk88 2 years ago
You are correct. Given answer is right.
upvoted 2 times

prabhjot 1 year, 11 months ago
yes azure Log analytics
upvoted 1 times

DSA_MSC Highly Voted 2 years, 11 months ago
A - YES
Same question: https://www.examtopics.com/discussions/microsoft/view/25631-exam-az-400-topic-7-question-4-discussion/
upvoted 16 times

[Removed] 2 years, 9 months ago
hmm good point. From MS perspective it is Log Analytics but in reality its KQL
upvoted 4 times

basw77 2 years, 2 months ago
You're right. Based on the other options from that question, we can conclude is should the correct answer is Log Analytics.
upvoted 2 times

OlehT Most Recent 2 months, 1 week ago
Selected Answer: A
Data analysis in Azure SQL Analytics is based on Log Analytics language. Period, do not overthink.
https://learn.microsoft.com/en-us/previous-versions/azure/azure-monitor/insights/azure-sql#analyze-data-and-create-alerts
upvoted 1 times

e0da014 3 months, 2 weeks ago

Topic 2, Question 10
You use Azure SQL Database Intelligent Insights and Azure Application Insights for monitoring.
You need to write ad-hoc queries against the monitoring data.
Which query language should you use?
A. Kusto Query Language (KQL) Most

Correct query language is Kusto
upvoted 1 times

Pillartech 5 months ago
A is the correct answer.
"Data analysis in Azure SQL Analytics is based on Log Analytics language for your custom querying and reporting."
https://learn.microsoft.com/en-us/previous-versions/azure/azure-monitor/insights/azure-sql#analyze-data-and-create-alerts
upvoted 2 times

saket051985 7 months, 3 weeks ago
While Azure Log Analytics is a powerful tool for analyzing and querying log data, it is not the primary tool for querying and analyzing data from Azure SQL Database Intelligent Insights and Azure Application Insights. Each of these services has its own query language.
Answer is B(No)
upvoted 1 times

Hgreg 9 months, 1 week ago
Selected Answer: A
"You need to utilize the correct query language."
"Solution: You use Azure Log Analytics." - This sentence does not say that Azure Log Analytics is a language. It simply says, that you use this service, which means that you use KQL. KQL is a correct answer, so I vote for A.
upvoted 2 times

kshk 10 months, 4 weeks ago
Selected Answer: B
Azure Log Analytics is not a query language. Kusto Query Language should be used for querying Application Insights and Azure Monitor. So, the correct answer is B.
upvoted 2 times

gabo 11 months, 3 weeks ago
It's asking for the query language, so only KQL can be the correct answer.
upvoted 1 times

flafernan 1 year ago
Selected Answer: B
The proposed solution for using Azure Log Analytics to analyze monitoring data from Azure SQL Database Intelligent Insights and Azure Application Insights does not meet the objective, as each of these tools has its own dedicated query languages (T-SQL and Kusto Query Language, respectively). Log Analytics is not an add-on tool for this specific type of analysis. So the correct answer is "No".
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: B
Should be yes when provided solution of this question is KQL (Kusto query language)
upvoted 1 times

itexamsmicrosoft 1 year, 2 months ago
Selected Answer: B
B. No
Azure Log Analytics is a service in Azure that provides comprehensive analytics and insights, not a query language itself. However, it uses Kusto Query Language (KQL), the same as Azure Application Insights and Azure SQL Database Intelligent Insights, for querying and analyzing the data. So, while Azure Log Analytics could potentially be part of a solution to analyze monitoring data, it isn't a query language as the question suggests. The correct query language for Azure Application Insights and Azure SQL Database Intelligent Insights is KQL.
upvoted 2 times

Architects 1 year, 2 months ago
A - log analytics and it use Kusto QL
upvoted 1 times

Rouix 1 year, 2 months ago

Here I would go for A - YES! You will utilize correct query language via Log Analytics Workspace and its Kusto Query Language.
upvoted 1 times

zellck 1 year, 3 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-query-overview
Azure Monitor Logs is based on Azure Data Explorer, and log queries are written by using the same Kusto Query Language (KQL). This rich language is designed to be easy to read and author, so you should be able to start writing queries with some basic guidance.
upvoted 3 times

yana_b 1 year, 3 months ago

Selected Answer: B

The primary query language used in Log Analytics is called Kusto Query Language (KQL)
upvoted 2 times

ShomaV 1 year, 3 months ago

Azure Application Insights, you would use the Application Insights Analytics query language. This query language is based on a subset of the Kusto Query Language (KQL) and allows you to perform advanced analytics and querying on your application telemetry data.
upvoted 1 times

Question #30 *Topic 1*

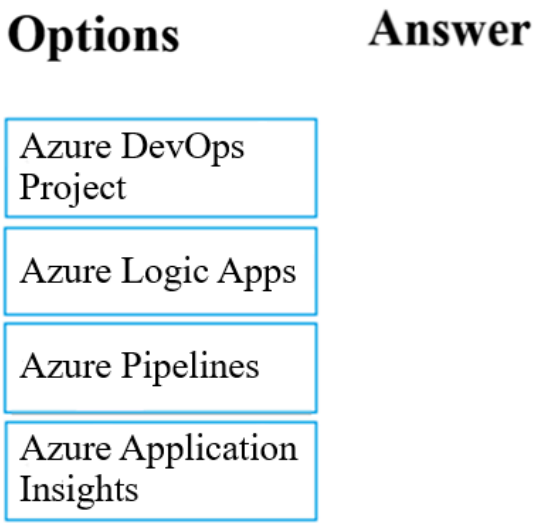
DRAG DROP -

You have recently created a web application for your company.

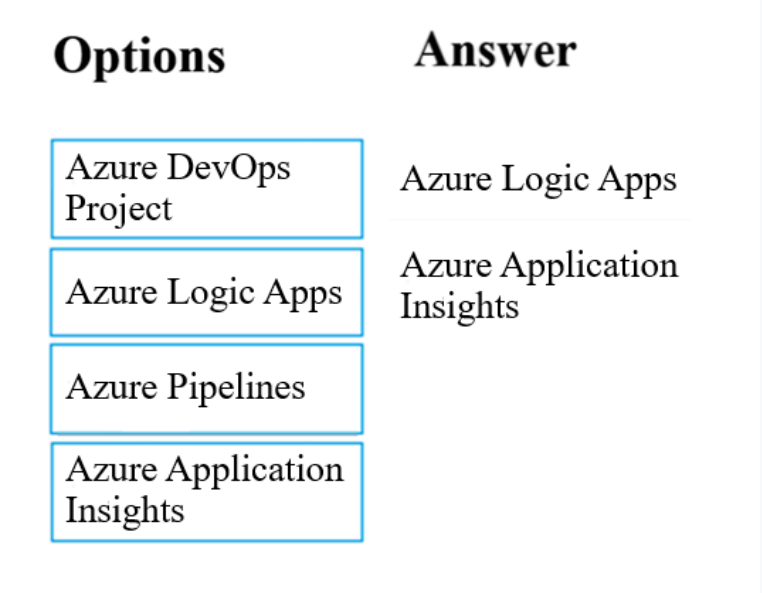
You have been tasked with making sure that a summary of the exceptions that transpire in the application is automatically sent to Microsoft Teams on a daily basis.

Which of the following Azure services should you use? Answer by dragging the correct options from the list to the answer area.

Select and Place:



Suggested Answer:



Exceptions in your live web app are reported by Application Insights.

Note: Periodical reports help keep a team informed on how their business critical services are doing. Developers, DevOps/SRE teams, and their managers can be productive with automated reports reliably delivering insights without requiring everyone to sign in the portal. Such reports can also help identify gradual increases in latencies, load or failure rates that may not trigger any alert rules.

You can programmatically query Application Insights data to generate custom reports on a schedule. The following options can help you get started quickly:

Automate reports with Microsoft Flow

▪

➪ Automate reports with Logic Apps

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/app/asp-net-exceptions https://docs.microsoft.com/en-us/azure/azure-monitor/app/automate-custom-reports

syu31svc Highly Voted 2 years, 1 month ago

https://docs.microsoft.com/en-us/azure/azure-monitor/app/automate-custom-reports

"Automate reports with Logic Apps"

Answer is correct
upvoted 14 times

petitbilly 1 year, 7 months ago
True, in here you can see that you need the logic app but also the connection to an App Insights resource: https://learn.microsoft.com/en-us/azure/azure-monitor/app/automate-with-logic-apps
upvoted 1 times

vsvaid Most Recent 8 months, 3 weeks ago
Correct answer
upvoted 1 times

yana_b 1 year, 1 month ago
AZ Logic Apps & AZ Application Insights
Provided answer is correct.
upvoted 2 times

zellck 1 year, 3 months ago
1. Azure Application Insights
2. Azure Logic Apps

https://learn.microsoft.com/en-us/previous-versions/azure/azure-monitor/app/custom-reports#automate-custom-report-emails
You can programmatically query Application Insights data to generate custom reports on a schedule. The following options can help you get started quickly:
- Automate reports with Azure Logic Apps.
upvoted 4 times

shamim_exam 1 year, 7 months ago
yup, given answer is correct
upvoted 1 times

Govcomm 2 years, 1 month ago
Azure Logic App (with the request trigger) and Azure Monitor action grouop.
upvoted 4 times

ccoutinho 2 years, 3 months ago
Sending the exceptions to MS Teams could also be done via a pipeline...
upvoted 2 times

memoor 1 year, 8 months ago
Stop misleading people please
upvoted 6 times

jvyas 2 years, 3 months ago
Given answer is correct.
https://docs.microsoft.com/en-us/azure/azure-monitor/app/automate-with-logic-apps
upvoted 1 times

Eltooth 2 years, 3 months ago
Logic apps
App Insights
upvoted 1 times

U3 2 years, 4 months ago
I think the answer is correct
upvoted 3 times

Question #31 *Topic 1*

You are in the process of building a mobile app aimed at Android and iOS devices.
All work items and release cycles are managed via Azure DevOps.
You want to make sure that crash reports for issue analysis is collected, and that beta releases are distributed to your testers. Also, you want to ensure that user feedback on the functionality of new apps is received.
Which of the following must be part of your solution?

A. The Microsoft Test & Feedback extension.

B. OWASP ZAP

C. TFS Integration Platform

D. Code Style

Suggested Answer: *A*
The "Exploratory Testing" extension is now "Test & Feedback" and is now Generally Available.
Anyone can now test web apps and give feedback, all directly from the browser on any platform: Windows, Mac, or Linux. Available for Google Chrome and
Mozilla Firefox (required version 50.0 or above) currently. Support for Microsoft Edge is in the pipeline and will be enabled once Edge moves to a Chromium- compatible web platform.
Reference:
https://marketplace.visualstudio.com/items?itemName=ms.vss-exploratorytesting-web

Community vote distribution

A (100%)

kapetan Highly Voted 3 years, 1 month ago
The question is regarding mobile apps, the answer should be Microsoft App Center, i.e. Visual Studio App Center.
upvoted 14 times

d0bermannn 2 years, 11 months ago
agreed
upvoted 1 times

murat12345 1 year, 11 months ago
I don't agree. With mobile development you can make use of emulators, which are applications on your pc that can be used with the test & feedback extension.
upvoted 1 times

Eltooth Highly Voted 2 years, 3 months ago
Selected Answer: A
A is only correct answer however if Visual Studio App Center is option then chose that one in exam.
upvoted 10 times

ozbonny Most Recent 6 months, 4 weeks ago
I think this can help to clarify why here the answer is A:

Integration with Microsoft Visual Studio App Center is a comprehensive solution that covers mobile app lifecycle management, including collecting bug reports, distributing beta versions, and obtaining user feedback. It is a robust option for teams looking for a complete solution for mobile app development and testing.

On the other hand, the Microsoft Test & Feedback extension is specifically designed to facilitate the collection of feedback and manual testing in web and desktop applications, but it can also be used for mobile applications. It allows collecting bug reports, distributing beta versions, and obtaining user feedback. It is an option more focused on the manual testing phase and collaboration between development teams and end users.
upvoted 3 times

varinder82 9 months, 3 weeks ago
A is only correct answer however if Visual Studio App Center is option then chose that one in exam.
upvoted 1 times

varinder82 9 months, 3 weeks ago

Final answer

Visual Studio App Center.

upvoted 1 times

yana_b 1 year, 1 month ago

Selected Answer: A

Correct answer

upvoted 1 times

karthikkarthik 1 year, 1 month ago

Selected Answer: A

Here option A makes more sense but there is a similar question that causes confusion:

https://www.examtopics.com/discussions/microsoft/view/16580-exam-az-400-topic-2-question-13-discussion/

upvoted 1 times

AbhishekGuptaHitk 1 year, 2 months ago

A is the Correct Answer

upvoted 1 times

zellck 1 year, 3 months ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/devops/test/perform-exploratory-tests?view=azure-devops

The Test & Feedback extension helps teams perform exploratory testing and provide feedback. Everyone in the team, such as developers, product owners, managers, UX or UI engineers, marketing teams, early adopters, and other stakeholders can use the extension to submit bugs or provide feedback and contribute to the quality of your product.

upvoted 3 times

mauryagrv 1 year, 7 months ago

Did not notice this in AZ400 docs, but the answer looks correct : A

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: A

https://docs.microsoft.com/en-us/azure/devops/test/perform-exploratory-tests?view=azure-devops:

"The Test & Feedback extension helps teams perform exploratory testing and provide feedback"

Answer is A

upvoted 5 times

Govcomm 2 years, 1 month ago

Correct, Microsoft Test and Feedback extension for IE or Chrome.

upvoted 2 times

Govcomm 2 years, 1 month ago

Correct, it is A.

upvoted 2 times

rdemontis 2 years, 5 months ago

Selected Answer: A

here the only possible solution with some sense is A, Microsoft Test & Feedback extension, even if for mobile apps you should use Visual Studio App Center.

upvoted 4 times

Sara_Mo 2 years, 7 months ago

A. The Microsoft Test & Feedback extension.

upvoted 3 times

yaytemur 3 years, 2 months ago

Correct.

upvoted 4 times

Question #1 *Topic 2*

DRAG DROP -

You need to recommend project metrics for dashboards in Azure DevOps.

Which chart widgets should you recommend for each metric? To answer, drag the appropriate chart widgets to the correct metrics. Each chart widget may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Chart Widgets	Answer Area	
Burndown	The elapsed time from the creation of work items to their completion:	
Cycle Time		
Lead Time	The elapsed time to complete work items once they are active:	
Velocity	The remaining work:	

Suggested Answer:

Chart Widgets	Answer Area	
Burndown	The elapsed time from the creation of work items to their completion:	Lead Time
Cycle Time		
Lead Time	The elapsed time to complete work items once they are active:	Cycle Time
Velocity	The remaining work:	Burndown

Box 1: Lead time -

Lead time measures the total time elapsed from the creation of work items to their completion.

Box 2: Cycle time -

Cycle time measures the time it takes for your team to complete work items once they begin actively working on them.

Box 3: Burndown -

Burndown charts focus on remaining work within a specific time period.

Incorrect Answers:

Velocity provides a useful metric for these activities:

Support sprint planning -

Forecast future sprints and the backlog items that can be completed

A guide for determining how well the team estimates and meets their planned commitments

Reference:

https://docs.microsoft.com/en-us/azure/devops/report/dashboards/velocity-guidance?view=vsts https://docs.microsoft.com/en-us/azure/devops/report/dashboards/cycle-time-and-lead-time?view=vsts https://docs.microsoft.com/en-us/azure/devops/report/dashboards/configure-burndown-burnup-widgets?view=vsts

AS007 Highly Voted 4 years, 4 months ago

Verified - its correct

upvoted 43 times

PaulMD 3 years, 4 months ago

Agreed. If you ever worked with JIRA, it's obvious ;)

upvoted 7 times

Sylph Highly Voted 3 years, 5 months ago

Lead Time: Lead time measures the total time elapsed from the creation of work items to their completion.

Cycle Time: Cycle time measures the time it takes for your team to complete work items once they begin actively working on them.

Burndown: Burndown charts focus on remaining work within a specific time period, while burnup charts focus on completed work.
https://docs.microsoft.com/en-us/azure/devops/report/dashboards/cycle-time-and-lead-time?view=azure-devops
https://docs.microsoft.com/en-us/azure/devops/report/dashboards/configure-burndown-burnup-widgets?view=azure-devops
upvoted 18 times

resonant Most Recent 1 year ago
I just got a question similar to this one today (September's 12th, 2023) but it asked something along the lines of what widget to use to show the count of results of a task query count and it was "Query Tile". One of the available options was "Query results" but the correct answer was "Query Tile".
upvoted 3 times

gabo 11 months, 3 weeks ago
Agree with you. Without proper knowledge, anyone would choose Query Results as the answer.
upvoted 2 times

yana_b 1 year, 1 month ago
Provided answer is correct
upvoted 1 times

olegjdll 1 year, 1 month ago
Here is good explaination of Cycle vs Lead time https://www.agile-academy.com/en/agile-dictionary/lead-time-vs-cycle-time/#:~:text=Definition%3A%20What%20are%20Lead%20Time,the%20request%20and%20deliver%20it.
upvoted 1 times

syu31svc 2 years, 1 month ago
https://docs.microsoft.com/en-us/azure/devops/report/dashboards/analytics-widgets?view=azure-devops

The Burndown widget lets you display a trend of remaining work
The Cycle Time widget will help you analyze the time it takes for your team to complete work items once they begin actively working on them
The Lead Time widget will help you analyze the time it takes to deliver work from your backlog

Answer is correct
upvoted 2 times

Govcomm 2 years, 1 month ago
Lead Time, Cycle Time and Velocity
upvoted 1 times

Govcomm 2 years, 1 month ago
Correction, Lead Time, Cycle and Burndown
upvoted 2 times

Eltooth 2 years, 3 months ago
Lead
Cycle
Burn down
upvoted 3 times

UnknowMan 2 years, 4 months ago
Correct
upvoted 1 times

rdemontis 2 years, 5 months ago
correct answer
upvoted 2 times

S1111_ 2 years, 6 months ago
was on exam today
upvoted 1 times

shermin1 2 years, 6 months ago
Came in exam march 13....
upvoted 1 times

esrojasbg 2 years, 6 months ago
Correcto!!

upvoted 1 times

durel 2 years, 7 months ago

Was good n the test feb 22

upvoted 1 times

durel 2 years, 7 months ago

Was good n the test feb 22

upvoted 2 times

Optimist_Indian 2 years, 7 months ago

Got this question in Feb-2022 (scored 910+). Given answer is correct.

upvoted 1 times

lugospod 2 years, 7 months ago

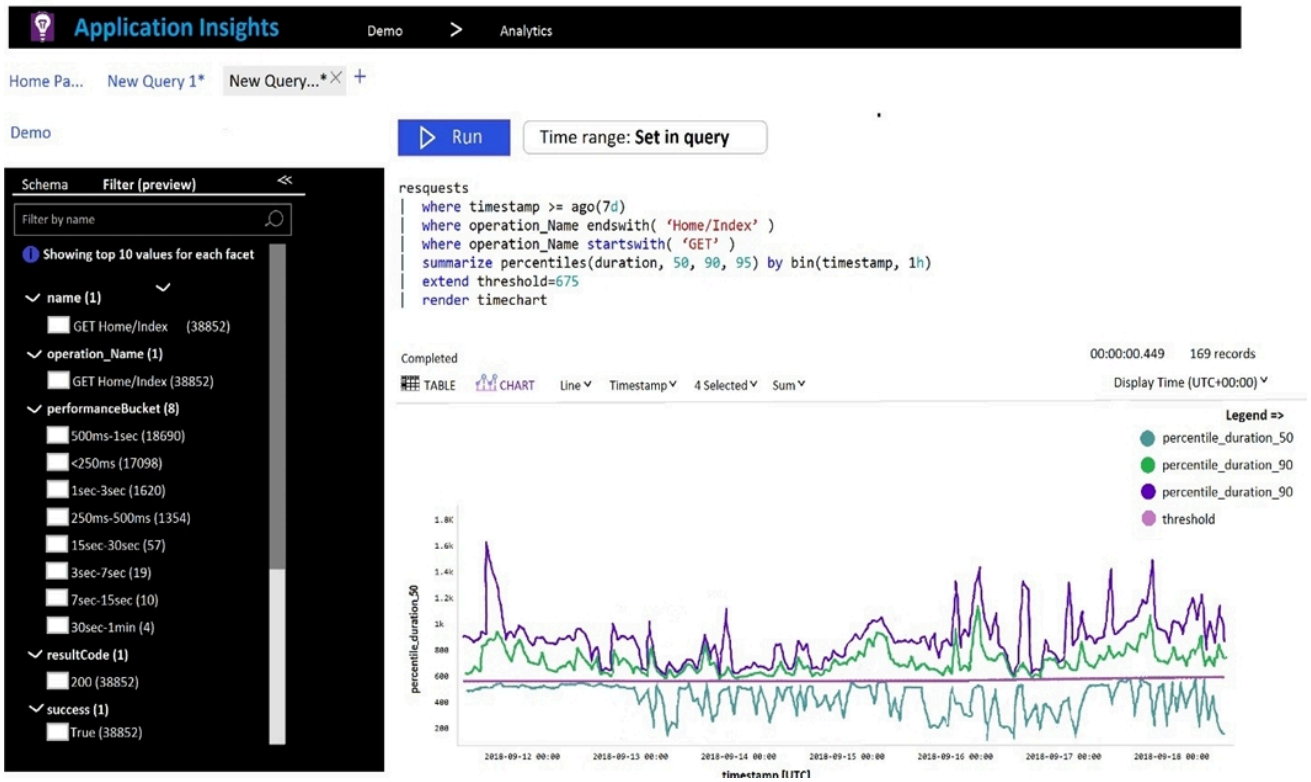
Got this January 2022.

upvoted 1 times

HOTSPOT -

You plan to create alerts that will be triggered based on the page load performance of a home page.

You have the Application Insights log query shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To create an alert based on the page load experience of most users, the alerting level must be based on **[answer choice]**.

- percentile_duration_50
- percentile_duration_90
- percentile_duration_95
- threshold

To only create an alert when authentication error occurs on the server, the query must be filtered on **[answer choice]**.

- item Type
- resultCode
- source
- success

Suggested Answer:

Answer Area

To create an alert based on the page load experience of most users, the alerting level must be based on **[answer choice]**.

- percentile_duration_50
- percentile_duration_90
- percentile_duration_95
- threshold

To only create an alert when authentication error occurs on the server, the query must be filtered on **[answer choice]**.

- item Type
- resultCode
- source
- success

Box 1: percentile_duration_95 -

Box 2: success -
For example ג€"
requests
| project name, url, success
| where success == "False"
This will return all the failed requests in my App Insights within the specified time range.
Reference:
https://devblogs.microsoft.com/premier-developer/alerts-based-on-analytics-query-using-custom-log-search/

Krastt Highly Voted 3 years, 5 months ago
I agree with the first answer, but the second one is not considering all scenarios.
In App Insight you can check the Request resultCode property which will show '403' in case of authentication errors. The answer for the second question should be 'resultCode' instead of 'success', as this will ensure that the error is strictly related to authentication.
upvoted 79 times

Nilf 3 years, 4 months ago
Not agree. On screenshot you can see only 1 Result Code - 200...
upvoted 7 times

prashanth364 1 year, 9 months ago
Based on your logic, it cant be success also, screenshot is not showing false for Success. So my answer is ResultCode as it clearly filters Authentication related errros
upvoted 3 times

nicksu 3 years, 2 months ago
It is also tracking 301 and 302, which aren't errors, obviously. But filtering on result oder would include them as well
upvoted 3 times

d0bermannn 3 years ago
it depends how to write a filter
upvoted 1 times

monniq Highly Voted 3 years, 4 months ago
I think the second answer should be resultCode. To detect authentication issue we're interested in 401 and 403. Success could be set to false not only due to authentication issue, but other issues like unhandled exceptions 500, and so on.
The first one is correct.
upvoted 36 times

d0bermannn 3 years ago
agreed, you may filter out all what to wish
upvoted 1 times

rdemontis 2 years, 6 months ago
agree with you

upvoted 3 times

chloaus Most Recent 5 months, 1 week ago

Percentile_duration_95

- This 95th percentile is the highest value left when the top 5% of a numerically sorted set of collected data is discarded.

Success

- Failed requests (requests/failed)

The count of tracked server requests that were marked as failed. By default, the Application Insights SDK automatically marks each server request that returned HTTP response code 5xx or 4xx as a failed request.

https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/app-insights-metrics

upvoted 2 times

saintnick 8 months, 4 weeks ago

Both answers are incorrect.

Answer 1 cannot be 95th percentile. That means you are creating an alert based on the response time that 5% of your users experience. The correct answer is 50th percentile. The threshold line even serves as a clue.

Answer 2 is not success because resultCode is a better option. The requirement is to identify authentication error and that information is held in the resultCode (401).

upvoted 1 times

sint822 9 months, 4 weeks ago

I think the second answer is wrong. Authentication error can be checked with Result Code (401 or 403 for example).

upvoted 1 times

WH16 1 year ago

On exam 2023-09-06, choose percentile_duration95 and resultCode.

Score 933

upvoted 9 times

yana_b 1 year, 1 month ago

Provided answer is correct

upvoted 3 times

all_cloud 1 year, 2 months ago

We need to return code to know why it has failed.

upvoted 3 times

mohiniu 1 year, 6 months ago

Answer should be result code , as we need alert only for authentication error only

upvoted 5 times

CaptainJameson 1 year, 7 months ago

Percentile has a good explanation on this page:

https://stackoverflow.com/questions/64928045/what-is-percentile-in-azure-metrics-web-app-slow#:~:text=They%20are%20the%20response%20time,take%201.5%20seconds%20or%20more.

In short: You want to base your alert on the load experience of most users. Percentile 95 is based on 95% of the data, which is more than 90% or 50%

upvoted 6 times

mmdex 1 year, 8 months ago

I see a lot of comments agreeing with the first answer, but no one cares to explain why. Is it really just a misunderstanding, as most (pun intended) people interpret the question as which query takes "the most" users into consideration (which is 95 of course)?

But the question is actually about "most" users, that is, more than 50%. And the percentile_duration_50 answer is also supported by the graph itself in my opinion - if you took either 90 or 95 percentile, you would be receiving alerts all the time as the duration is constantly above threshold.

upvoted 6 times

Wengatz 1 year, 8 months ago

50, 90, and 95 would all be acceptable answers for an interpretation of "most users" as "at least 50% of users". If you interpret it as "most all users", 95 would be the best answer here. If I say "most people agree that the Earth is round", chances are, I mean to say that most everyone agrees this. It's a poorly worded question.

upvoted 3 times

FNog 1 year, 6 months ago
We shall not overthink it. 95% it is.
upvoted 1 times

Fal991l 1 year, 5 months ago
GPT: Percentile_duration_50 represents the median page load time, which is the value that separates the upper half from the lower half of the page load times. This means that 50% of the page loads are faster than the median value and 50% are slower. Therefore, using the median value as the basis for the alerting level would be a good indicator of the page load experience of most users.

On the other hand, percentile_duration_95 represents the page load time for the 95th percentile of the users, which is the threshold at which only 5% of the users are experiencing longer page load times. While this can also be a useful metric to monitor, it may not be representative of the page load experience of most users.
upvoted 4 times

budha 1 year, 9 months ago
It was on my exam on December 7, 2022.
upvoted 4 times

hart232 1 year, 9 months ago
Which answer did you select?
upvoted 1 times

Atos 2 years ago
Could not understand this question until i realised the purple line is meant to be 95. So top answer is correct.
Bottom answer should be result code; then you can select codes such as 401.
upvoted 3 times

sindhu2693 2 years, 1 month ago
For second option, question clearly states to filter for authentication error, and the apt option would be based on result codes, but not success
upvoted 3 times

syu31svc 2 years, 1 month ago
Alert based on most users is 95th percentile is for sure

Alert based on authentication is success; either pass or fail

Answer to me is correct
upvoted 1 times

tjeerd 2 years, 1 month ago
On exam 20220727. Choose 95 percentile and resultCode.
upvoted 5 times

Govcomm 2 years, 1 month ago
percent_tile_95 and resultCode are the right answer.
upvoted 3 times

Question #3 *Topic 2*

You manage an Azure web app that supports an e-commerce website.
You need to increase the logging level when the web app exceeds normal usage patterns. The solution must minimize administrative overhead.
Which two resources should you include in the solution? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. an Azure Automation runbook

B. an Azure Monitor alert that has a dynamic threshold

C. an Azure Monitor alert that has a static threshold

D. the Azure Monitor autoscale settings

E. an Azure Monitor alert that uses an action group that has an email action

Suggested Answer: *AB*
B: Metric Alert with Dynamic Thresholds detection leverages advanced machine learning (ML) to learn metrics' historical behavior, identify patterns and anomalies that indicate possible service issues. It provides support of both a simple UI and operations at scale by allowing users to configure alert rules through the Azure
Resource Manager API, in a fully automated manner.
A: You can use Azure Monitor to monitor base-level metrics and logs for most services in Azure. You can call Azure Automation runbooks by using action groups or by using classic alerts to automate tasks based on alerts.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-dynamic-thresholds https://docs.microsoft.com/en-us/azure/automation/automation-create-alert-triggered-runbook

Community vote distribution
AB (100%)

Dalias Highly Voted 3 years, 2 months ago
got this in 30 Jun 2021 exams. scored 800+ marks. answer is right
upvoted 23 times

SriLen Highly Voted 3 years, 7 months ago
Given Answer is correct
upvoted 21 times

alirezak22 Most Recent 2 months, 1 week ago
Selected Answer: AB
AB are correct
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: AB
Correct
upvoted 2 times

renzoku 1 year, 2 months ago
Selected Answer: AB
B. Azure Monitor alert that has a dynamic threshold.
alerts is adjust based on "exceeds normal usage patterns"(dynamic threshold)

A. Azure Automation runbook.
Script that can be executed when specific conditions are met(Azure Monitor Alert) and increases the logging level.

Azure Monitor alert that uses an action group that has an email action, we need adjust the logging level not send an email.
upvoted 6 times

mauryagrv 1 year, 7 months ago

AB is correct
upvoted 1 times

aadi369 1 year, 7 months ago
Selected Answer: AB
Ans is AB
upvoted 1 times

AvinashVarma 1 year, 8 months ago
Azure Automation runbook and Azure Monitor alert that has a dynamic threshold are correct answers.
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: AB
"minimize administrative overhead"

A is one of the answers for sure

https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-dynamic-thresholds;
"Metric Alert with Dynamic Thresholds detection leverages advanced machine learning (ML)'

B is the answer since ML would reduce overhead ain't it?
upvoted 2 times

Govcomm 2 years, 1 month ago
Azure Monitor Dynamic threshold and Azure Automation Account to increase the logging level.
upvoted 1 times

Leandrocei 2 years, 2 months ago
Correct. Came today 22 july 9
upvoted 2 times

Eltooth 2 years, 3 months ago
Selected Answer: AB
A & B are correct answers.
upvoted 2 times

RoadRunner97 2 years, 4 months ago
Action groups can send an alert to a automation runbook via webhook, which will increase logging level of webapp via code. I believe AB are the correct answers.
upvoted 2 times

rdemontis 2 years, 5 months ago
Selected Answer: AB
Correct answer
upvoted 1 times

rajvelm 2 years, 10 months ago
Came in today 5th Nov 2021
upvoted 2 times

sabrinaAm 3 years, 1 month ago
can anyone explain to met how azure runbook is a correct answer ?
upvoted 5 times

ukkuru 3 years, 1 month ago
To send alert why not we we use manage action groups:
https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups#:~:text=An%20action%20group%20is%20a,an%20alert%20has%20been%20triggered.
upvoted 1 times

Swwapnil 2 years, 12 months ago
as they said , administrative overhead must be minimized so this would not be preferred answer
upvoted 1 times

HOTSPOT -

You have an Azure Kubernetes Service (AKS) pod.

You need to configure a probe to perform the following actions:

- ✑ Confirm that the pod is responding to service requests.
- ✑ Check the status of the pod four times a minute.
- ✑ Initiate a shutdown if the pod is unresponsive.

How should you complete the YAML configuration file? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
apiVersion: v1
kind: Pod
metadata:
     labels:
          test: readiness-and-liveness
     name: readiness-http
spec:
     containers:
     - name: container1
       image: k8s.gcr.io/readiness-and-liveness
       args:
       - /server
```

[▼]
- livenessProbe:
- readinessProbe:
- ShutdownProbe:
- startupProbe:

```
    httpGet:
         path: /checknow
         port: 8123
         httpHeaders:
         - name: Custom-Header
           value: CheckNow
```

[▼]
- initialDelaySeconds: 15
- periodSeconds: 15
- timeoutSeconds: 15

Suggested Answer:

Answer Area

```
apiVersion: v1
kind: Pod
metadata:
     labels:
          test: readiness-and-liveness
     name: readiness-http
spec:
     containers:
     - name: container1
       image: k8s.gcr.io/readiness-and-liveness
       args:
       - /server
```

livenessProbe:
readinessProbe:
ShutdownProbe:
startupProbe:

```
    httpGet:
         path: /checknow
         port: 8123
         httpHeaders:
         - name: Custom-Header
           value: CheckNow
```

initialDelaySeconds: 15
periodSeconds: 15
timeoutSeconds: 15

Box 1: readinessProbe:
For containerized applications that serve traffic, you might want to verify that your container is ready to handle incoming requests. Azure Container Instances supports readiness probes to include configurations so that your container can't be accessed under certain conditions.
Incorrect Answers:
livenessProbe: Containerized applications may run for extended periods of time, resulting in broken states that may need to be repaired by restarting the container. Azure Container Instances supports liveness probes so that you can configure your containers within your container group to restart if critical functionality is not working.

Box 2: periodSeconds: 15 -
The periodSeconds property designates the readiness command should execute every 15 seconds.
Reference:
https://docs.microsoft.com/en-us/azure/container-instances/container-instances-readiness-probe

k8smaster Highly Voted 3 years, 2 months ago
The readinessProbe is wrong.
It clearly says "Initiate a shutdown if the pod is unresponsive."
How can you iniate a shutdown (restart) with readinessProbe.
It must have been livelinessProbe.
upvoted 87 times

Tranquillo1811 1 year, 10 months ago
The real question is, what "Shutdown" actually means:
a) restart the container
b) remove the pod from the SLB
upvoted 1 times

rdemontis 2 years, 5 months ago
Agree with you. Here the question asks to initiate a shutdown if the pod is unresponsive. Shutdown means that the process will be killed and then restarted. It's different from a simple restart.
"If the process in your container is able to crash on its own whenever it encounters an issue or becomes unhealthy, you do not necessarily need a liveness probe; the kubelet will automatically perform the correct action in accordance with the Pod's restartPolicy.
If you'd like your container to be killed and restarted if a probe fails, then specify a liveness probe, and specify a restartPolicy of Always or OnFailure"

https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle/#container-probes

upvoted 4 times

jperona Highly Voted 3 years, 2 months ago

The correct answer is liveness because you want that your POD restart in case of failure.
Readiness remove the POD from Load Balancer, but doesn't restart it.

The kubelet uses liveness probes to know when to restart a container. For example, liveness probes could catch a deadlock, where an application is running, but unable to make progress. Restarting a container in such a state can help to make the application more available despite bugs.

The kubelet uses readiness probes to know when a container is ready to start accepting traffic. A Pod is considered ready when all of its containers are ready. One use of this signal is to control which Pods are used as backends for Services. When a Pod is not ready, it is removed from Service load balancers.

upvoted 65 times

d0bermannn 3 years ago

best comment here

upvoted 7 times

sondrex Most Recent 2 months, 3 weeks ago

1. livenessProbe: Ensures the container is running. If the liveness probe fails, Kubernetes will kill the container and restart it
2. initialDelaySeconds: 15

upvoted 3 times

4bd3116 4 months, 4 weeks ago

The correct answer is livenessProbe, and periodSeconds: 15 :
apiVersion: v1
kind: Pod
metadata:
name: my-aks-pod
spec:
containers:
- name: my-app-container
image: my-app-image
ports:
- containerPort: 80
livenessProbe:
httpGet:
path: /healthz
port: 80
initialDelaySeconds: 15
periodSeconds: 15
failureThreshold: 3

upvoted 2 times

FeriAZ 5 months, 4 weeks ago

Liveness Probes
Period Seconds: 15

upvoted 2 times

vsvaid 8 months, 3 weeks ago

Liveness Probes
Period Seconds; 15

Liveness Probes are used to check if the pod is responding or not. If not reboot.

Readiness probe is used to check if the pod is ready to accept request.

upvoted 1 times

sint822 9 months, 4 weeks ago

livelinessProbe is correct. readinessProbe is for checking container dependencies and seeing if services are ready for serve request.

upvoted 1 times

yana_b 1 year, 1 month ago

Readiness probe & period seconds:15
upvoted 4 times

omerco61 1 year, 3 months ago
I quote in microsoft official site;

Readines Probes;
For containerized applications that serve traffic, you might want to verify that your container is ready to handle incoming requests.

liveness probes;
Azure Container Instances supports liveness probes so that you can configure your containers within your container group to restart if critical functionality is not working.

Answers;
Liveness Probes
Period Seconds; 15
upvoted 2 times

Fal991l 1 year, 5 months ago
yaml code (GPT):

livenessProbe:
httpGet:
path: /Server
port: <port number>
initialDelaySeconds: 15
periodSeconds: 15
timeoutSeconds: 15
failureThreshold: 4
upvoted 1 times

Vmwarevirtual 1 year, 6 months ago
The provided answers are correct - check the definition regarding containers probe types - https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle/#container-probes
upvoted 3 times

syu31svc 2 years, 1 month ago
https://docs.microsoft.com/en-us/azure/container-instances/container-instances-readiness-probe

https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle/

"readinessProbe
Indicates whether the container is ready to respond to requests"

"Confirm that the pod is responding to service requests" (From question)

I would agree with the given answer
upvoted 3 times

syu31svc 2 years ago
Sorry disregard my earlier answer

Is liveness as per what the rest have mentioned
upvoted 2 times

Govcomm 2 years, 1 month ago
liveness to reboot when the system is unresponsive. Readness is when the system ready to accepts the requests.
upvoted 2 times

Eltooth 2 years, 3 months ago
Liveness
Period seconds 15

upvoted 5 times

ben_t 2 years, 3 months ago

I agree with liveness probe, it is described here https://cloud.google.com/blog/products/containers-kubernetes/kubernetes-best-practices-setting-up-health-checks-with-readiness-and-liveness-probes

But it is Microsoft tests and all will be possible. One can observe metadata where you can find the name of pod =) It is related to readyness.

upvoted 1 times

UnknowMan 2 years, 4 months ago

liveness is most appropriate (Kill the process)

upvoted 1 times

Sara_Mo 2 years, 8 months ago

The correct answer

Box1: Liveness Probe

Box2:Period seconds 15

upvoted 5 times

Question #5 *Topic 2*

You have a Microsoft ASP.NET Core web app in Azure that is accessed worldwide.
You need to run a URL ping test once every five minutes and create an alert when the web app is unavailable from specific Azure regions. The solution must minimize development time.
What should you do?

A. Create an Azure Monitor Availability metric and alert.

B. Create an Azure Application Insights availability test and alert.

C. Write an Azure function and deploy the function to the specific regions.

D. Create an Azure Service Health alert for the specific regions.

Suggested Answer: *B*
There are three types of Application Insights availability tests:
URL ping test: a simple test that you can create in the Azure portal.
▪
➪ Multi-step web test
➪ Custom Track Availability Tests
Note: After you've deployed your web app/website, you can set up recurring tests to monitor availability and responsiveness. Azure Application Insights sends web requests to your application at regular intervals from points around the world. It can alert you if your application isn't responding, or if it responds too slowly.
You can set up availability tests for any HTTP or HTTPS endpoint that is accessible from the public internet. You don't have to make any changes to the website you're testing. In fact, it doesn't even have to be a site you own. You can test the availability of a REST API that your service depends on.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/monitor-web-app-availability#create-a-url-ping-test

Community vote distribution
B (100%)

dimitartachev23 Highly Voted 3 years, 5 months ago
Correctamundo dude
upvoted 23 times

goatlord 3 years, 1 month ago
Yes, my dude.
upvoted 8 times

AlMargoi 2 years, 9 months ago
Indeed dudes
upvoted 3 times

omw2wealth 2 years, 9 months ago
Exactly DUDES
upvoted 2 times

PlumpyTumbler 2 years, 8 months ago
Be excellent to each other dudes.
upvoted 2 times

bamibi 2 years, 3 months ago
why does it feel like ive stumbed onto a reddit thread
upvoted 12 times

DoctorCOmputer 2 years, 4 months ago
Dudes be come dude
upvoted 1 times

JSTech 2 years, 1 month ago
Appreciate it dude and dudets

upvoted 2 times

alirezak22 Most Recent 2 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

yana_b 1 year, 1 month ago

Selected Answer: B

Provided answer is correct

upvoted 2 times

omerco61 1 year, 3 months ago

Selected Answer: B

B Correct

Check article;
https://learn.microsoft.com/en-us/azure/azure-monitor/app/availability-overview#:~:text=After%20you%27ve%20deployed,responds%20too%20slowly.

After you've deployed your web app or website, you can set up recurring tests to monitor availability and responsiveness. Application Insights sends web requests to your application at regular intervals from points around the world. It can alert you if your application isn't responding or responds too slowly.

upvoted 1 times

syu31svc 2 years, 1 month ago

B for sure

"Monitor availability with URL ping tests"
"To create an availability test, you need use an existing Application Insights resource or create an Application Insights resource."

Straight from the link given

upvoted 3 times

Govcomm 2 years, 1 month ago

Application insights Availability test.

upvoted 1 times

AIM2H 2 years, 2 months ago

B is the right answer

upvoted 1 times

Eltooth 2 years, 3 months ago

Selected Answer: B

B is correct answer.

upvoted 2 times

rdemontis 2 years, 5 months ago

Selected Answer: B

correct

upvoted 2 times

S1111_ 2 years, 6 months ago

was on exam today

upvoted 2 times

christianMa 2 years, 6 months ago

Selected Answer: B

right answer

upvoted 2 times

shermin1 2 years, 6 months ago

Came in exam march 13....

upvoted 2 times

durel 2 years, 7 months ago

Was in the test feb 22

upvoted 2 times

durel 2 years, 7 months ago

Was in the test feb 22

upvoted 1 times

ar407 2 years, 7 months ago

Dude, where's my Azure Application Insights availability test?

upvoted 3 times

Question #6 *Topic 2*

You have a multi-tier application. The front end of the application is hosted in Azure App Service.
You need to identify the average load times of the application pages.
What should you use?

A. Azure Application Insights

B. the activity log of the App Service

C. the diagnostics logs of the App Service

D. Azure Advisor

Suggested Answer: *A*
Application Insights will tell you about any performance issues and exceptions, and help you find and diagnose the root causes.
Application Insights can monitor both Java and ASP.NET web applications and services, WCF services. They can be hosted on-premises, on virtual machines, or as Microsoft Azure websites.
On the client side, Application Insights can take telemetry from web pages and a wide variety of devices including iOS, Android, and Windows Store apps.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/web-monitor-performance

Community vote distribution

A (100%)

27close Highly Voted 3 years, 10 months ago
you can get the performance data (duration) from Application insight..
https://docs.microsoft.com/en-us/azure/devops/test/load-test/get-performance-data-for-load-tests?view=azure-devops
upvoted 14 times

alirezak22 Most Recent 2 months, 1 week ago
Selected Answer: A
A is correct.
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: A
Azure Application Insights
upvoted 2 times

geekdamsel 1 year, 5 months ago
Got this question in exam. Right answer is Azure Application Insights.
upvoted 1 times

Jawad1462 1 year, 10 months ago
Selected Answer: A
Correct
upvoted 1 times

syu31svc 2 years, 1 month ago
A for sure; others are invalid
upvoted 1 times

Govcomm 2 years, 1 month ago
Azure Application Insights for the load time.
upvoted 1 times

Eltooth 2 years, 3 months ago
Selected Answer: A
A is correct answer.
upvoted 1 times

UnknowMan 2 years, 4 months ago

Selected Answer: A

Correct

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: A

correct

upvoted 2 times

shermin1 2 years, 6 months ago

Came in exam march 13....

upvoted 3 times

durel 2 years, 7 months ago

Was in the test feb 22

upvoted 3 times

lugospod 2 years, 7 months ago

Got this January 2022 - Insight (got 100% on that part)

upvoted 3 times

Sara_Mo 2 years, 8 months ago

Given answer is correct

upvoted 1 times

Mage10 2 years, 9 months ago

Selected Answer: A

correct

upvoted 2 times

AravindhGS 2 years, 10 months ago

Selected Answer: A

Given answer is correct

upvoted 2 times

DrewL 3 years, 1 month ago

correct answer, use application insights to view the load

upvoted 2 times

SIMULATION -

You need to create an instance of Azure Application Insights named az400-123456789-main and configure the instance to receive telemetry data from an Azure web app named az400-123456789-main.

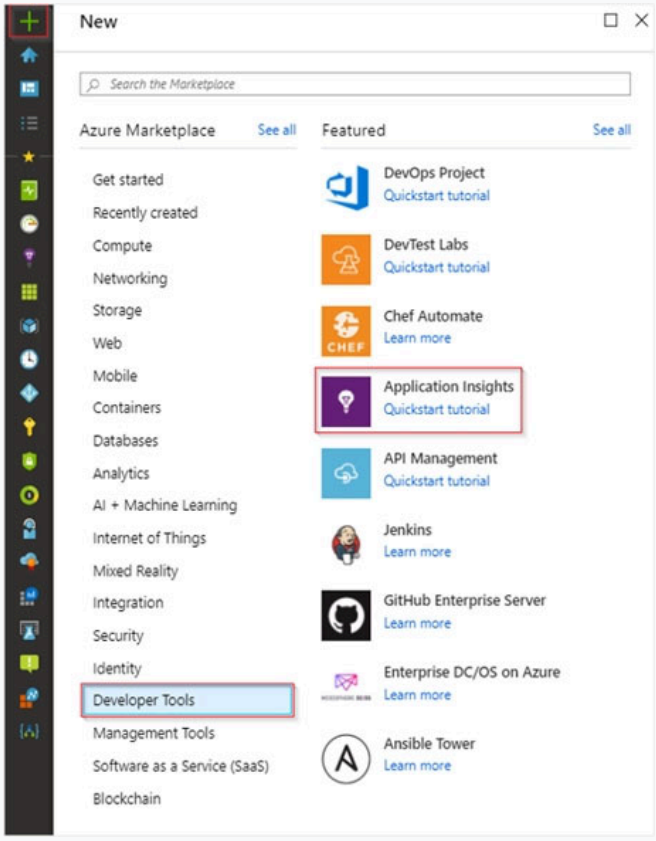
To complete this task, sign in to the Microsoft Azure portal.

Suggested Answer: *See explanation below.*

Step 1: Create an instance of Azure Application Insights

1. Open Microsoft Azure Portal

2. Log into your Azure account, Select Create a resource > Developer tools > Application Insights.



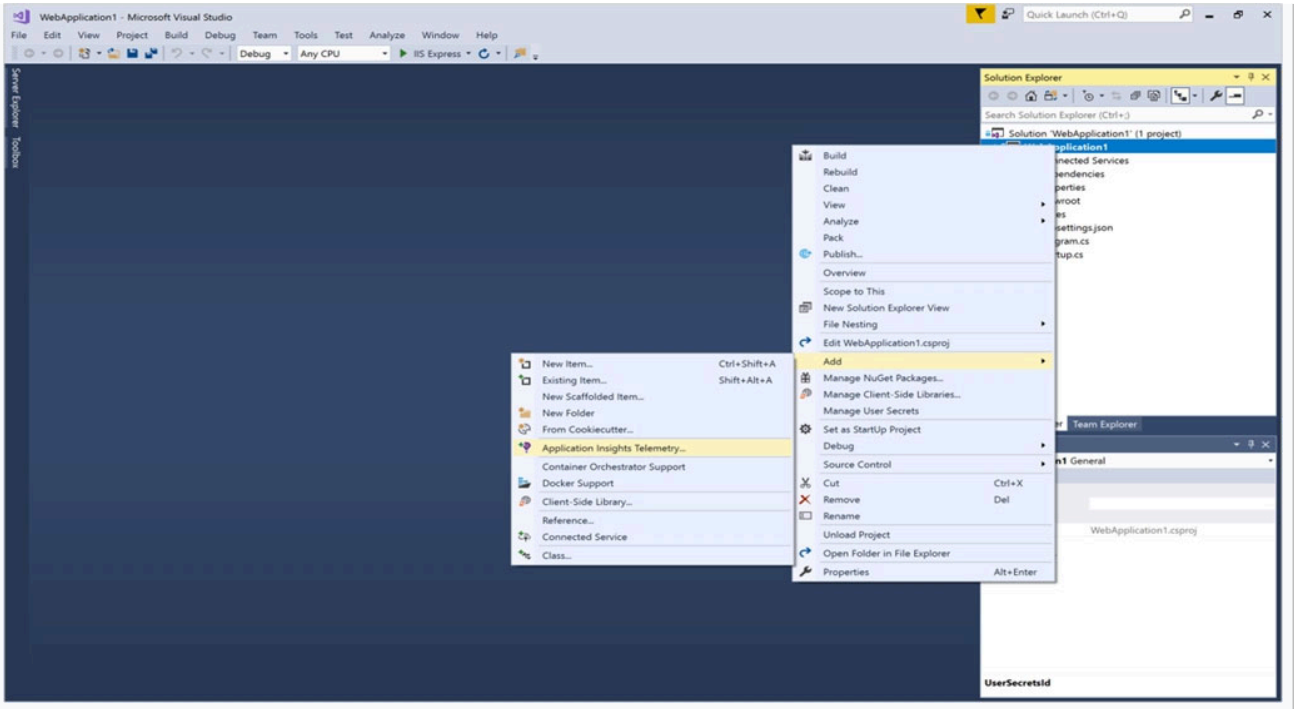
3. Enter the following settings, and then select Review + create.

Name: az400-123456789-main -

Step 2: Configure App Insights SDK

1. Open your ASP.NET Core Web App project in Visual Studio > Right-click on the AppName in the Solution Explorer > Select Add > Application Insights

Telemetry.



2. Click the Get Started button

3. Select your account and subscription > Select the Existing resource you created in the Azure portal > Click Register.

Reference:

https://docs.microsoft.com/bs-latn-ba/azure/azure-monitor/learn/dotnetcore-quick-start?view=vs-2017

giuliohome Highly Voted 2 years ago

it's an azure web app so you go there in app services and Select Application Insights in the Azure control panel for your app service, then select Enable.

https://docs.microsoft.com/en-us/azure/azure-monitor/app/azure-web-apps-nodejs?tabs=windows#auto-instrumentation-through-azure-portal

BTW It's nowhere written it is a dotnet app

upvoted 20 times

buzzerboy 1 year, 7 months ago

I did the samething for azure web app also.

upvoted 1 times

xRiot007 Highly Voted 1 year, 1 month ago

You need to enable App Insights for an Azure App. It has nothing to do with Visual Studio.

Your steps:

1. Login to Az Portal
2. Create an App Insights resource
3. Locate your Az Web App, if it does not exist, create it.
4. Go to the resource, to Settings, to Application Insights and enable it. Select the App Insights resource you created earlier and Apply.

This should be all.

upvoted 11 times

chakanirban Most Recent 2 months, 3 weeks ago

NO LAB on 6/21 - 9 am IST -

1 Case study , 6 new Q

1 YES NO series was new - 3 Q - I answered all No , because 2 will No and 1 Y

JOB A depends JOB B

JOB B on JOB C

JOB C on JOB D

who is dependent , who can run parallel

3 yes/ no

upvoted 6 times

karthikwarrior 3 months ago

I took exam today from home, there were no simulations (lab) only one case study!
upvoted 4 times

chakanirban 2 months, 3 weeks ago
yes, u were my inspiration and got no labs
upvoted 1 times

sibishrewd 7 months, 3 weeks ago
got this lab in today's exam but VS was not installed in my lab
upvoted 3 times

Kem81 1 year ago
are there simulations in the real exam? I thought they removed them.
upvoted 6 times

yana_b 1 year, 1 month ago
Try this sequence of steps and you will enable the Apps insights for a web app via the AZ Portal:
1. Login to AZ portal
2. Create new resource -> search for Application insights -> create new (use the instance name in the lab)
3. Create new resource -> Web app (uncheck application insights)
4. Once both resources are depolyed => go to the web app
5. Under Settings click on Application Insights -> enable -> mark 'Select an existing resource'
6. click on the Application insights created in step 2 -> Apply
Provided solution in the question itself refers to enabling App Insights in Visual studio
upvoted 3 times

zeaimen 1 year, 2 months ago
I don't get this part : Open your ASP.NET Core Web App project in Visual Studio : where is this VS supposed to be?
upvoted 1 times

zellck 1 year, 3 months ago
Gotten this in Jun 2023 exam.
upvoted 3 times

gabo 11 months, 3 weeks ago
so how do you do this in the exam? Do you get a Azure portal to login? What about credentials?
upvoted 1 times

xda 7 months, 2 weeks ago
Got this on my exam too (January2024)
Credentials will be provided from the exam. Its a real Azure-Webportal.
upvoted 2 times

__srey1212 7 months, 1 week ago
Did you follow the instructions that is there in the discussion section?
upvoted 1 times

ShivaUdari 1 year, 7 months ago
Can use Azure portal and achieve the goal to enable insights for Azure Web App
upvoted 1 times

Question #8 *Topic 2*

Your company uses ServiceNow for incident management.
You develop an application that runs on Azure.
The company needs to generate a ticket in ServiceNow when the application fails to authenticate.
Which Azure Log Analytics solution should you use?

A. Application Insights Connector

B. Automation & Control

C. IT Service Management Connector (ITSM)

D. Insight & Analytics

Suggested Answer: *C*
The IT Service Management Connector (ITSMC) allows you to connect Azure and a supported IT Service Management (ITSM) product/service.
ITSMC supports connections with the following ITSM tools:
➪ ServiceNow
➪ System Center Service Manager
➪ Provance
➪ Cherwell

With ITSMC, you can -
➪ Create work items in ITSM tool, based on your Azure alerts (metric alerts, Activity Log alerts and Log Analytics alerts).
➪ Optionally, you can sync your incident and change request data from your ITSM tool to an Azure Log Analytics workspace.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/itsmc-overview

Community vote distribution

C (100%)

Cluster007 Highly Voted 3 years, 10 months ago
Correct
upvoted 12 times

Kem81 Most Recent 1 year ago
Same type of question in the AZ-104 exam. Answer it the ITSM connector.
upvoted 2 times

yana_b 1 year, 1 month ago
Selected Answer: C
Correct answer
upvoted 1 times

budha 1 year, 9 months ago
It was on my exam on December 7, 2022.
upvoted 2 times

syu31svc 2 years, 1 month ago
Selected Answer: C
ServiceNow is ITSM so answer is C for sure
upvoted 1 times

Govcomm 2 years, 1 month ago
ITSM with ServiceNow
upvoted 1 times

Eltooth 2 years, 3 months ago
Selected Answer: C
C is correct answer.

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: C

correct

upvoted 1 times

novac1111 2 years, 7 months ago

Selected Answer: C

Correct

upvoted 2 times

CodePoet 2 years, 8 months ago

Selected Answer: C

Correct answer

upvoted 4 times

Aniruddha_dravyakar 2 years, 11 months ago

answer is correct

upvoted 1 times

27close 3 years, 10 months ago

Create work items in your ITSM tool, based on your Azure alerts (metric alerts, activity log alerts, and Log Analytics alerts).
Optionally, you can sync your incident and change request data from your ITSM tool to an Azure Log Analytics workspace.

upvoted 2 times

27close 3 years, 10 months ago

IT Service Management Connector (ITSMC) allows you to connect Azure to a supported IT Service Management (ITSM) product or service.

upvoted 4 times

Question #9 *Topic 2*

HOTSPOT -

Your company is building a new web application.

You plan to collect feedback from pilot users on the features being delivered.

All the pilot users have a corporate computer that has Google Chrome and the Microsoft Test & Feedback extension installed. The pilot users will test the application by using Chrome.

You need to identify which access levels are required to ensure that developers can request and gather feedback from the pilot users. The solution must use the principle of least privilege.

Which access levels in Azure DevOps should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Developers: [ ] ▼
- Basic
- Stakeholder

Pilot users: [ ] ▼
- Basic
- Stakeholder

Suggested Answer:

Answer Area

Developers: [ ] ▼
- Basic
- Stakeholder

Pilot users: [ ] ▼
- Basic
- Stakeholder

Box 1: Basic -

Assign Basic to users with a TFS CAL, with a Visual Studio Professional subscription, and to users for whom you are paying for Azure Boards & Repos in an organization.

Box 2: Stakeholder -

Assign Stakeholders to users with no license or subscriptions who need access to a limited set of features.

Note:

You assign users or groups of users to one of the following access levels:

Basic: provides access to most features

VS Enterprise: provides access to premium features

Stakeholders: provides partial access, can be assigned to unlimited users for free

Reference:

https://docs.microsoft.com/en-us/azure/devops/organizations/security/access-levels?view=vsts

faltu1985 Highly Voted 4 years, 4 months ago

Yes, I think answers are correct, please ignore my last message

upvoted 48 times

yayh Highly Voted 4 years, 4 months ago

answers are correct

upvoted 33 times

yana_b Most Recent 1 year, 1 month ago
Developers -> basic
Pilot users -> stake holders
upvoted 1 times

KumaTed 1 year, 3 months ago
The Provided Answer is correct
upvoted 1 times

iabhi10 1 year, 6 months ago
Given answer is correct
Statement from azure doc :-
Only users with Basic access can request feedback. Basic users can provide feedback using the flow described in this topic.
upvoted 1 times

Mcphyl 1 year, 9 months ago
The Provided Answer is correct
Box 1 = Basic
Only users with Basic can request feedback and remember Basic access level is Higher than Stakeholder access level

Box 2: Stakeholders access level is enough to provide feedback Going by the principle of least privilege

https://learn.microsoft.com/en-us/azure/devops/organizations/security/access-levels?view=azure-devops#supported-access-levels

https://learn.microsoft.com/en-us/azure/devops/test/request-stakeholder-feedback?view=azure-devops

https://learn.microsoft.com/en-us/azure/devops/test/connected-mode-exploratory-testing?view=azure-devops#prerequisites
upvoted 5 times

mrg998 1 year, 7 months ago
yaas queen
upvoted 3 times

dotnet_dev 1 year, 9 months ago
Developer: Stakeholders
Pilot users: Basic

References here: https://learn.microsoft.com/en-us/azure/devops/organizations/security/access-levels?view=azure-devops
upvoted 1 times

Anjana30 1 year, 11 months ago
Yes , the given answer is correct
upvoted 1 times

Tranquillo1811 1 year, 11 months ago
I think it should be
Stakeholder
Stakeholder

see reference here:
https://learn.microsoft.com/en-us/azure/devops/test/connected-mode-exploratory-testing?view=azure-devops
Under "Prerequisites" section: "To request or provide feedback, you must have Stakeholder access or higher."
upvoted 4 times

murat12345 1 year, 11 months ago
I agree with that. Not sure why other people claim that devs need to have basic access.

"To request or provide feedback, you must have Stakeholder access or higher."
upvoted 1 times

murat12345 1 year, 11 months ago
But on this page "https://learn.microsoft.com/en-us/azure/devops/test/request-stakeholder-feedback?view=azure-devops" it says "Only users with Basic access can request feedback."... so not sure what the answer is. Anyone?

upvoted 1 times

syu31svc 2 years, 1 month ago

https://docs.microsoft.com/en-us/azure/devops/test/connected-mode-exploratory-testing?view=azure-devops

"Users with Basic access can use the extension to perform exploratory testing, as described below.

Users with Stakeholder access can use the extension to respond to feedback requests or to provide feedback voluntarily."

Answer is correct

upvoted 1 times

Govcomm 2 years, 1 month ago

Developer: Basic

Pilot users: Stakeholders

upvoted 1 times

Leandrocei 2 years, 2 months ago

Correct. Came today 22 july 9

upvoted 1 times

Eltooth 2 years, 3 months ago

Basic

Stakeholder

upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 2 times

S1111_ 2 years, 6 months ago

was on exam today

upvoted 2 times

rdemontis 2 years, 6 months ago

Given answers are correct!

https://docs.microsoft.com/en-us/azure/devops/test/request-stakeholder-feedback?view=azure-devops

upvoted 2 times

shermin1 2 years, 6 months ago

Came in exam march 13....

upvoted 2 times

Question #10 *Topic 2*

You use Azure SQL Database Intelligent Insights and Azure Application Insights for monitoring.
You need to write ad-hoc queries against the monitoring data.
Which query language should you use?

A. Kusto Query Language (KQL)

B. PL/pgSQL

C. PL/SQL

D. Transact-SQL

Suggested Answer: *A*
Azure Monitor Logs is based on Azure Data Explorer, and log queries are written using the same Kusto query language (KQL). This is a rich language designed to be easy to read and author, and you should be able to start using it with minimal guidance.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-query-overview

Community vote distribution

A (100%)

dtodorov Highly Voted 3 years, 3 months ago
Correct
upvoted 14 times

goatlord Highly Voted 3 years, 1 month ago
Big Correct
upvoted 7 times

yana_b Most Recent 1 year, 1 month ago
Selected Answer: A
Kusto Query Language (KQL)
upvoted 1 times

omerco61 1 year, 3 months ago
Correct Dudes.
upvoted 1 times

Radul85 1 year, 7 months ago
Correct !
upvoted 1 times

EAGERTOLEARN 1 year, 9 months ago
Correct. Kusto Query Language (KQL)
upvoted 1 times

Matharax 1 year, 11 months ago
Kusto is the correct query language to be used.
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: A
Azure Monitor Logs is based on Azure Data Explorer, and log queries are written using the same Kusto query language (KQL).

100% is A
upvoted 1 times

Govcomm 2 years, 1 month ago
KQL: Kusto Query Language
upvoted 1 times

Eltooth 2 years, 3 months ago

Selected Answer: A

A is correct answer.

upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 1 times

Squadra 2 years, 4 months ago

Correct

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: A

correct

upvoted 2 times

Mev4953 2 years, 7 months ago

Selected Answer: A

Correct

upvoted 3 times

Pankaj78 2 years, 9 months ago

Selected Answer: A

correct

upvoted 3 times

Question #11 *Topic 2*

Your company creates a web application.
You need to recommend a solution that automatically sends to Microsoft Teams a daily summary of the exceptions that occur in the application.
Which two Azure services should you recommend? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Azure Logic Apps

B. Azure Pipelines

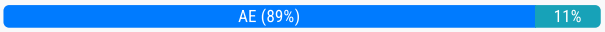
C. Microsoft Visual Studio App Center

D. Azure DevOps Project

E. Azure Application Insights

Suggested Answer: *AE*
E: Exceptions in your live web app are reported by Application Insights.
Note: Periodical reports help keep a team informed on how their business critical services are doing. Developers, DevOps/SRE teams, and their managers can be productive with automated reports reliably delivering insights without requiring everyone to sign in the portal. Such reports can also help identify gradual increases in latencies, load or failure rates that may not trigger any alert rules.
A: You can programmatically query Application Insights data to generate custom reports on a schedule. The following options can help you get started quickly:
➪ Automate reports with Microsoft Flow
➪ Automate reports with Logic Apps
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/asp-net-exceptions https://docs.microsoft.com/en-us/azure/azure-monitor/app/automate-custom-reports

Community vote distribution



jacyang Highly Voted 4 years, 2 months ago
The given answer is correct.
upvoted 28 times

PM2 Highly Voted 4 years ago
Correct.Verified.
upvoted 8 times

ozbonny Most Recent 6 months, 4 weeks ago
Selected Answer: AE
A. Azure Logic Apps
E. Azure Application Insights
upvoted 2 times

yana_b 1 year, 1 month ago
Selected Answer: AB
Logic Apps and Az Application Insights
upvoted 2 times

syu31svc 2 years, 1 month ago
Selected Answer: AE
https://docs.microsoft.com/en-us/azure/azure-monitor/app/automate-custom-reports

"Automate reports with Logic Apps"

A and E are the answers
upvoted 2 times

Govcomm 2 years, 1 month ago

Azure Logic Apps with Azure Application Insights

upvoted 2 times

Eltooth 2 years, 3 months ago

Selected Answer: AE

A & E are correct answers.

upvoted 2 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 2 times

Mcelona 2 years, 4 months ago

Selected Answer: AE

The given answer is correct

upvoted 2 times

rdemontis 2 years, 6 months ago

Give answer is correct

https://docs.microsoft.com/en-us/azure/azure-monitor/app/automate-with-logic-apps

upvoted 1 times

shermin1 2 years, 6 months ago

Came in exam march 13....

upvoted 2 times

durel 2 years, 7 months ago

Was in the test feb 22

upvoted 2 times

novac1111 2 years, 7 months ago

Selected Answer: AE

the given answer is correct

upvoted 2 times

lugospod 2 years, 7 months ago

Got this January 2022

upvoted 1 times

Pankaj78 2 years, 9 months ago

Selected Answer: AE

The given answer is correct.

upvoted 3 times

MartijnSchoemaker 2 years, 9 months ago

Selected Answer: AE

Correct

upvoted 3 times

AZ5cert 2 years, 12 months ago

Correct Answer

Azure Insight Reports can send by

- Power automate
- Logic apps

https://docs.microsoft.com/en-us/azure/azure-monitor/app/automate-custom-reports

upvoted 2 times

Question #12 *Topic 2*

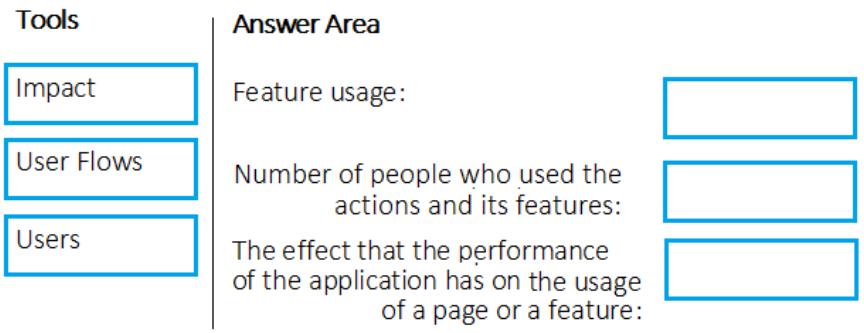
DRAG DROP -

Your company wants to use Azure Application Insights to understand how user behaviors affect an application.

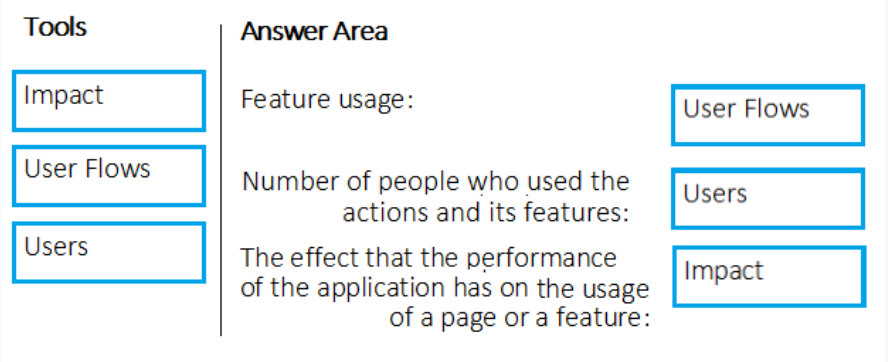
Which Application Insights tool should you use to analyze each behavior? To answer, drag the appropriate tools to the correct behaviors. Each tool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested Answer:



Box 1: User Flows -

The User Flows tool visualizes how users navigate between the pages and features of your site. It's great for answering questions like:

How do users navigate away from a page on your site?

What do users click on a page on your site?

Where are the places that users churn most from your site?

Are there places where users repeat the same action over and over?

Box 2: Users -

Counting Users: The user behavior analytics tools don't currently support counting users or sessions based on properties other than anonymous user ID, authenticated user ID, or session ID.

Box 3: Impact -

Impact analyzes how load times and other properties influence conversion rates for various parts of your app. To put it more precisely, it discovers how any dimension of a page view, custom event, or request affects the usage of a different page view or custom event.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/app/usage-flows https://docs.microsoft.com/en-us/azure/azure-monitor/app/usage-impact https://docs.microsoft.com/en-us/azure/azure-monitor/app/usage-troubleshoot

TosO Highly Voted 4 years, 6 months ago

Feature usage -> Users

User action by day -> User Flows

The effect ... -> Impact

upvoted 131 times

dan7777 4 years ago

Totally agree.

upvoted 3 times

TrangNguyen_6 2 years, 11 months ago
You are correct!
Users tool: How many people used your app and its features. Users are counted by using anonymous IDs stored in browser cookies. A single person using different browsers or machines will be counted as more than one user.
upvoted 4 times

thetrapt 4 years, 5 months ago
@TosO is right.
Feature usage -> Users. https://docs.microsoft.com/en-us/azure/azure-monitor/app/usage-segmentation
User action by day -> User Flows. https://docs.microsoft.com/en-us/azure/azure-monitor/app/usage-flows
The effect ... -> Impact
upvoted 8 times

hubeau 4 years, 5 months ago
Because your articles, i think the anwser is correct. I met a similar question in az-203.
User acion by day -> users

The User Flows tool visualizes how users navigate between the pages and features
upvoted 9 times

hubeau 4 years, 5 months ago
Feature usage -> User Flows
User action by day -> Users

Your link is not convinced @thetrapt

The User Flows tool visualizes how users navigate between the pages and features of your site. It's great for answering questions like:
How do users navigate away from a page on your site?
What do users click on a page on your site?
Where are the places that users churn most from your site?
Are there places where users repeat the same action over and over?
upvoted 27 times

chaudh 4 years, 3 months ago
Feature usage -> User Flows. https://docs.microsoft.com/en-us/azure/azure-monitor/app/usage-flows --> Special Session Started nodes show where the subsequent nodes began a session. Session Ended nodes show how many users sent no page views or custom events after the preceding node, highlighting where users probably left your site.
User action by day -> Users. https://docs.microsoft.com/en-us/azure/azure-monitor/app/usage-segmentation --> allow "Querying for certain users"
The effect ... -> Impact
upvoted 10 times

rdemontis 2 years, 5 months ago
totally agree with you. provided answer is correct
upvoted 2 times

Atanu Highly Voted 4 years, 2 months ago
Answer is correct
upvoted 25 times

e0da014 Most Recent 3 months, 2 weeks ago
Provided answer is correct

Number of people who used actions and it's feature : Users (Refer this: https://learn.microsoft.com/en-us/azure/azure-monitor/app/usage-segmentation)
Users tool: How many people used your app and its features? Users are counted by using anonymous IDs stored in browser cookies. A single person using different browsers or machines will be counted as more than one user.
upvoted 3 times

resonant 1 year ago
Got a question similar to this (September's 12th, 2023), but I was asked what should I use to know how often are certain pages and features of your app used or something like that and the answer is Events.
upvoted 5 times

d365ppp 1 year ago
I am really surprised users on this site randomly post on discussions. Looks like they neither have any experience nor had read the training materials. posting wrong answers and cluttering the site.
upvoted 1 times

yana_b 1 year, 1 month ago
1. Feature usage -> User Flows -> evidence: https://learn.microsoft.com/en-us/azure/azure-monitor/app/usage-flows
2. No of people -> Users -> evidenced by: https://learn.microsoft.com/en-us/azure/azure-monitor/app/usage-segmentation#the-users-sessions-and-events-segmentation-tool
3. The effect of the performance to page usage -> Impact -> evidenced by: https://learn.microsoft.com/en-us/azure/azure-monitor/app/usage-impact
upvoted 2 times

zellck 1 year, 3 months ago
1. User Flows
2. Users
3. Impact

https://learn.microsoft.com/en-us/azure/azure-monitor/app/usage-flows
The User Flows tool visualizes how users move between the pages and features of your site.

https://learn.microsoft.com/en-us/azure/azure-monitor/app/usage-segmentation#the-users-sessions-and-events-segmentation-tool

https://learn.microsoft.com/en-us/azure/azure-monitor/app/usage-impact
Impact analyzes how load times and other properties influence conversion rates for various parts of your app. To put it more precisely, it discovers how any dimension of a page view, custom event, or request affects the usage of a different page view or custom event.
upvoted 3 times

surensaluka 1 year, 7 months ago
This came today for my exam on 2023-02-14. Selected the @TosO's answer.
upvoted 5 times

rahul51it 1 year, 7 months ago
Thanks
upvoted 1 times

Yatoom 1 year, 10 months ago
The second item doesn't read "User action by day", it reads "Number of people who used the actions and its features". So the answer should be "Users", right?

In that case, it should be:
- Users
- Users
- Impact
upvoted 3 times

Jis247 1 year, 11 months ago
Users tool:-
How many people used your app and its features. Users are counted by using anonymous IDs stored in browser cookies. A single person using different browsers or machines will be counted as more than one user.

The User Flows tool visualizes:---
how users navigate between the pages and features of your site. It's great for answering questions like:

How do users navigate away from a page on your site?
What do users click on a page on your site?
Where are the places that users churn most from your site?
Are there places where users repeat the same action over and over?
upvoted 1 times

Darkeh 1 year, 12 months ago
This is one of those "can you read" type of questions. I hope I get more of these on the test.

upvoted 1 times

AmjadAli 2 years, 1 month ago

Correct Answer

upvoted 1 times

syu31svc 2 years, 1 month ago

https://docs.microsoft.com/en-us/azure/azure-monitor/app/usage-segmentation
https://docs.microsoft.com/en-us/azure/azure-monitor/app/usage-impact
https://docs.microsoft.com/en-us/azure/azure-monitor/app/usage-flows

I would agree with the answer given

upvoted 1 times

Govcomm 2 years, 1 month ago

User Flows, Users and Impact

upvoted 1 times

Divyayuvi 2 years, 2 months ago

1. User Flows
2. User Flows
3. Impact

upvoted 1 times

Inland 2 years, 3 months ago

Given answers are correct.
https://dailydotnettips.com/user-flows-in-application-insights/
https://docs.microsoft.com/en-us/azure/azure-monitor/app/tutorial-users

upvoted 1 times

Eltooth 2 years, 3 months ago

Obsolete question now as new Users, Sessions and Event Analysis segmentation tool covers these.
https://docs.microsoft.com/en-us/azure/azure-monitor/app/usage-segmentation

If pushed for an answer:
User Flow
Users
Impact

upvoted 2 times

Question #13 *Topic 2*

Your company is building a mobile app that targets Android and iOS devices.
Your team uses Azure DevOps to manage all work items and release cycles.
You need to recommend a solution to perform the following tasks:
➪ Collect crash reports for issue analysis.
➪ Distribute beta releases to your testers.
➪ Get user feedback on the functionality of new apps.
What should you include in the recommendation?

A. the Microsoft Test & Feedback extension

B. Microsoft Visual Studio App Center integration

C. Azure Application Insights widgets

D. Jenkins integration

Suggested Answer: *A*
The "Exploratory Testing" extension is now "Test & Feedback" and is now Generally Available.
Anyone can now test web apps and give feedback, all directly from the browser on any platform: Windows, Mac, or Linux. Available for Google Chrome and
Mozilla Firefox (required version 50.0 or above) currently. Support for Microsoft Edge is in the pipeline and will be enabled once Edge moves to a Chromium- compatible web platform.
Reference:
https://marketplace.visualstudio.com/items?itemName=ms.vss-exploratorytesting-web

Community vote distribution
B (100%)

TosO Highly Voted 4 years, 6 months ago
The answer is B.
For mobile, it is always Microsoft Visual Studio App Center
upvoted 121 times

thetrapt 4 years, 5 months ago
Right. https://visualstudio.microsoft.com/app-center/
upvoted 11 times

hubeau 4 years, 5 months ago
Yes

2. Start the SDK
Open AppDelegate.swift file and add the following lines below your own import statements.

import AppCenter
import AppCenterAnalytics
import AppCenterCrashes
In the same file, add the following in your didFinishLaunchingWithOptions delegate method.

MSAppCenter.start("2b17e7b3-f7d8-4f72-8245-48d873b9ed6e", withServices:[
MSAnalytics.self,
MSCrashes.self
])
upvoted 5 times

magdi 3 years, 11 months ago
this is from MS docs
Manage your email preferences to sign up for automatic notifications for builds, distributions, and crashes.
upvoted 3 times

lolit Highly Voted 4 years, 5 months ago
TosO is right -- answer is B. But WHY are there so many fake answers here??
upvoted 21 times

Alexevansigg 3 years, 11 months ago
The guys supplying the questions are experts in stealing exam question... not experts in answering them.
upvoted 61 times

MarsMoon 3 years, 6 months ago
Yes, But atleast they are providing for free. So you should be thankful to examtopics.
upvoted 34 times

DiligentAmoeba 1 year, 1 month ago
totally agree...
Let this be a positive community :)
upvoted 2 times

[Removed] 3 years, 9 months ago
LOOOOOOOL
upvoted 6 times

LouisD 3 years, 6 months ago
I think this is so that people don't just go in and brain dump the questions, but actually have to figure it out.
upvoted 4 times

coffecold 1 year, 10 months ago
Right, my impression as well..
upvoted 1 times

UrbanRellik Most Recent 2 months, 4 weeks ago
Selected Answer: B
B. Microsoft Visual Studio App Center.

Soon to be deprecated... (3/31/2025)
upvoted 2 times

InversaRadice 4 months, 4 weeks ago
The answer is correct 100% and u are all wrong.
upvoted 1 times

1sadad 5 months ago
Pretty sure this is out of scope for the AZ400 now, nothing in the learning path on microsoft learn on this.
upvoted 1 times

FeriAZ 6 months, 2 weeks ago
Selected Answer: B
A. Microsoft Test & Feedback extension: This extension is primarily for providing feedback on web applications within Visual Studio, not ideal for mobile app testing and crash reporting.
B. Microsoft Visual Studio App Center integration: This service offers features specifically designed for mobile app development, including:
Crash reporting: Collects and analyzes crash reports from Android and iOS devices.
Distribution: Manages beta releases and distributes builds to testers for various platforms (Android, iOS).
User feedback: Enables testers to provide feedback directly within the app through surveys and bug reports.
upvoted 1 times

ozbonny 6 months, 4 weeks ago
Selected Answer: B
I'll go by B
upvoted 1 times

wolfyzawolf 11 months, 1 week ago
Users, User Flows, Impact

Feature Usage:
Tool: Users
Explanation: The "Users" tool helps in analyzing the usage of different features within the application by different users over time. This tool will

help in understanding how often certain features are being used and by how many users.

Number of users who used the actions and its features:
Tool: User Flows
Explanation: The "User Flows" tool provides insight into the paths users take through your application. It can be utilized to see the sequence of actions users take including which features they interact with, and in what order.

The effect that the performance of the application has on the usage of a page or a feature:
Tool: Impact
Explanation: The "Impact" tool analyzes how performance metrics affect user behavior. For instance, it can help understand how the load time of a page or a feature affects its usage, thus providing insights into areas where performance optimizations can enhance user experience.
upvoted 1 times

yana_b 1 year, 1 month ago

Selected Answer: B

Visual Studio App Center lets you automate and manage the lifecycle of your iOS, Android, Windows, and macOS apps. Ship apps more frequently, at higher-quality, and with greater confidence. Connect your repo and within minutes automate your builds, test on real devices in the cloud, distribute apps to beta testers, and monitor real-world usage with crash and analytics data. All in one place.

https://visualstudio.microsoft.com/app-center/faq/
https://visualstudio.microsoft.com/app-center/
https://learn.microsoft.com/en-us/appcenter/build/
upvoted 1 times

karthikkarthik 1 year, 1 month ago

Selected Answer: B

I think the answer is "B. Microsoft Visual Studio App Center integration" but a similar question that was previously asked confused me:
https://www.examtopics.com/discussions/microsoft/view/57280-exam-az-400-topic-1-question-31-discussion/
upvoted 3 times

Pavlo 1 year, 3 months ago

B Microsoft Visual Studio App Center integration, and Azure Application Insights widgets.
upvoted 1 times

Pukun 1 year, 3 months ago

B. Microsoft Visual Studio App Center integration
upvoted 1 times

ShomaV 1 year, 3 months ago

Azure DevOps provides integration with various crash reporting tools, such as App Center Crash Analytics, App Center Distribute. For collecting feedback use Azure DevOps integration with UserVoice
upvoted 1 times

jimmyyml 1 year, 7 months ago

From ChatGpt,
The recommended solution for collecting crash reports, distributing beta releases, and getting user feedback for a mobile app targeting Android and iOS devices using Azure DevOps is Microsoft Visual Studio App Center integration.

B. Microsoft Visual Studio App Center provides a suite of services and tools for mobile app development and management, including crash reporting, beta distribution, and user feedback. It integrates seamlessly with Azure DevOps, allowing teams to manage their mobile app development and releases in one place.

A. The Microsoft Test & Feedback extension is a tool for exploratory testing and feedback collection, but it does not provide crash reporting or beta distribution features.

C. Azure Application Insights widgets are used for monitoring web applications and do not provide crash reporting or beta distribution features for mobile apps.

D. Jenkins is a tool for continuous integration and delivery and does not provide features for crash reporting, beta distribution, or user feedback collection for mobile apps.

Therefore, the correct answer is:

B. Microsoft Visual Studio App Center integration

upvoted 6 times

MeMoToTe 1 year, 2 months ago

If you ask chatgpt again, it will answer differently. It's not even have up-to-date information

upvoted 1 times

Yagna_Dev 1 year, 7 months ago

Microsoft test and feedback extension is for browsers. App center is for Ios,Android etc

upvoted 2 times

richat 1 year, 7 months ago

not able to access page 40 in exam topic as free?

upvoted 1 times

AlexLiourtas 1 year, 7 months ago

it used to be free, for the past year or so you gotta pay for the rest. imho it is worth it.

upvoted 1 times

sradev 1 year, 8 months ago

Topic 1 Question #31, same question , answer 100% - A. The Microsoft Test & Feedback extension.

?????

upvoted 5 times

surensaluka 1 year, 8 months ago

You're correct. In that question, AppCenter wasn't in the answer choices.

upvoted 2 times

Question #14 *Topic 2*

You have an Azure DevOps project named Project1 and an Azure subscription named Sub1. Sub1 contains an Azure virtual machine scale set named VMSS1.
VMSS1 hosts a web application named WebApp1. WebApp1 uses stateful sessions.
The WebApp1 installation is managed by using the Custom Script extension. The script resides in an Azure Storage account named sa1.
You plan to make a minor change to a UI element of WebApp1 and to gather user feedback about the change.
You need to implement limited user testing for the new version of WebApp1 on VMSS1.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Modify the load balancer settings of VMSS1.

B. Redeploy VMSS1.

C. Upload a custom script file to sa1.

D. Modify the Custom Script extension settings of VMSS1.

E. Update the configuration of a virtual machine in VMSS1.

Suggested Answer: *BCD*

Community vote distribution

CDE (94%) 6%

TosO Highly Voted 4 years, 5 months ago
Answer: CDE

Not Correct:
A - Statefull sessions are already configured
B - If you redeploy the VMSS1, the new configuration will apply to all virtual machines. "The requirement is: You need to implement limited user testing for the new version of WebApp1 on VMSS1."
upvoted 85 times

temporal111 4 years ago
In my opinion you are correct, to reinforce your answer:
https://medium.com/charot/custom-script-extention-on-azure-vmss-e010a8c87904 Here we can find a simple explanation of why isn't necessary the redeploy step
upvoted 3 times

OhBee 4 years, 4 months ago
Certain modifications may be applied to specific VMs instead of the global scale set properties. Currently, the only VM-specific update that is supported is to attach/detach data disks to/from VMs in the scale set. This feature is in preview. For more information, see the preview documentation.

https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-upgrade-scale-set
upvoted 2 times

OhBee 4 years, 4 months ago
What I meant by this is that I am not sure if E is correct here...
upvoted 3 times

Alexevansigg 3 years, 11 months ago
If you change the settings for the VMSS (ie set a new custom script extension) That script can be applied to a subset of instances if you have auto-upgrade disabled. Applying an Upgrade to a VMSS Instance is the same as 'Update the Configuration of a VM' So Answer is CDE.
upvoted 4 times

kcinofni 4 years, 4 months ago
Completely agree. We cannot modify appropriately settings of the scale set load balancer, as well as we cannot install extensions directly to particular scale set instance.

upvoted 2 times

nagendra25may Highly Voted 4 years, 2 months ago

Answer is ACD.

Explanation:-

Upload the changes to Storage Account.

Change The extension script to deploy the changes only to few VMs.

Change Load Balancer to distribute the traffic to new changes vs old changes and see the feedback.

upvoted 34 times

UnknowMan 2 years, 4 months ago

Cant be A because of Stateful session

upvoted 1 times

omw2wealth 2 years, 9 months ago

No, i trust TosO.

Answer: CDE

upvoted 5 times

jmwania 1 year, 1 month ago

You're right.

upvoted 1 times

FeriAZ Most Recent 6 months, 2 weeks ago

Selected Answer: CDE

C. Upload a custom script file to sa1: Since WebApp1 installation and updates are managed by the Custom Script extension, you need to modify the script in your Azure storage account (sa1) with the new version that includes the UI change.

D. Modify the Custom Script extension settings of VMSS1: This allows you to point the extension to the updated script location in sa1, triggering the installation of the new WebApp1 version with the UI change on all VMs within the VMSS1 scale set.

E. Update the configuration of a virtual machine in VMSS1: While this might seem tempting, it's crucial to remember that VMSS1 is a scale set. Updating a single VM configuration wouldn't update the entire set, and you might end up with an inconsistent environment.

upvoted 3 times

mohiniu 1 year, 6 months ago

It seems it can be done in 2 ways:

Option1 :

C. Upload a custom script file to sa1.

Upload new script with newer version of code.

D. Modify the Custom Script extension settings of VMSS1.

Point Scaleset to new script in storage account

E. Update the configuration of a virtual machine in VMSS1.

Increase number of VMS in scaleset from say 3 to 4. With this change , new VM VM-4 will be having newer code. And first 3 VMS will continue to run with older version of code.

Option2:

C. Upload a custom script file to sa1.

Upload new script with newer version of code.

[F] Create a new scaleset and point this scaleset to new script

A. Modify the load balancer settings of VMSS1.

Update loadbalancer settings such that traffic is distributed between new and older scaleset.

As , we are not having option [F] in the answer. CDE should be right answer.

upvoted 7 times

Ak1009 1 year, 7 months ago

Selected Answer: ACD

Chat GPT Says ACD

E : Option E ("Update the configuration of a virtual machine in VMSS1") is not a necessary step to implement limited user testing for the new version of WebApp1 on VMSS1, so it is not a correct answer in this case.

Updating the configuration of a virtual machine in the scale set would only be necessary if you wanted to make specific changes to that virtual machine, such as changing its size, its network configuration, or its OS disk image. However, if you want to implement limited user testing on the web application running on all virtual machines in the scale set, you would typically use the Custom Script extension or another deployment method to update the code running on all the virtual machines at once, rather than modifying the configuration of each virtual machine individually.

I believe A is necessary for Canary testing as we want to test it for just limited number of Users.
upvoted 1 times

Fal991l 1 year, 5 months ago
another version from gpt:
To implement limited user testing for the new version of WebApp1 on VMSS1, you should perform the following three actions:

B. Redeploy VMSS1: To deploy the new version of WebApp1, you need to update the VMSS with the new code. This can be achieved by redeploying VMSS1.

C. Upload a custom script file to sa1: To make the minor UI changes to WebApp1, you need to modify the custom script file that is used to manage the installation of WebApp1. You can upload the updated script file to the Azure Storage account named sa1.

D. Modify the Custom Script extension settings of VMSS1: After updating the custom script file, you need to modify the settings of the Custom Script extension of VMSS1 to use the updated script file during the redeployment process.

Therefore, the correct options are:

B. Redeploy VMSS1.
C. Upload a custom script file to sa1.
D. Modify the Custom Script extension settings of VMSS1.
upvoted 1 times

friendlyvlad 1 year, 9 months ago
The answer is CDE. A and B are simply not related. We do not need to make any changes to the scaleset to deploy a small UI change. The rest was explained in Update App deployment section of https://learn.microsoft.com/en-us/azure/virtual-machine-scale-sets/tutorial-install-apps-powershell.
upvoted 2 times

stevenzo 1 year, 9 months ago
You can still load balance with stateful sessions.
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: CDE
https://cloudblogs.microsoft.com/opensource/2018/06/18/tutorial-canary-deployment-for-azure-virtual-machine-scale-sets/

Answer is CDE
upvoted 6 times

srine69 1 year, 12 months ago
Great reference
upvoted 1 times

Rams_84zO6n 1 year, 6 months ago
CDE
Canary deployment -> Update the configuration of a virtual machine in VMSS1 - emphasis on "a virtual machine"
upvoted 1 times

Govcomm 2 years, 1 month ago
Update the configuration
Custom Script Extension
Update the VMSS
upvoted 1 times

marras 2 years, 3 months ago

Selected Answer: CDE

CDE based on this link: After research I've found this link: https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/tutorial-install-apps-powershell (section "Update app deployment") where they show update steps:

```
$vmss = Get-AzVmss `
-ResourceGroupName "myResourceGroup" `
-VMScaleSetName "myScaleSet"

$vmss.VirtualMachineProfile.ExtensionProfile[0].Extensions[0].Settings = $customConfigv2

Update-AzVmss `
-ResourceGroupName "myResourceGroup" `
-Name "myScaleSet" `
-VirtualMachineScaleSet $vmss
```

upvoted 1 times

UnknowMan 2 years, 4 months ago

Selected Answer: CDE

CDE do the job

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: CDE

IMHO canary deployment could be a good solution for this scenario because we have to implement limited user testing for the new version of WebApp1 on VMSS1. So correct answer should be C,D,E

upvoted 1 times

AM11 2 years, 7 months ago

Selected Answer: CDE

Refer this post.
https://cloudblogs.microsoft.com/opensource/2018/06/18/tutorial-canary-deployment-for-azure-virtual-machine-scale-sets/

upvoted 2 times

jay158 2 years, 5 months ago

Best reference to clarify the answer CDE

upvoted 1 times

debanjan10 2 years, 9 months ago

Selected Answer: CDE

Correct answer is CDE

upvoted 1 times

d0bermannn 2 years, 12 months ago

if use a logic must be a\c\e

upvoted 4 times

d0bermannn 3 years ago

ACE looks logical, with A as a must part of solution for affected vm isolation

upvoted 3 times

DeepMoon 3 years, 6 months ago

C- Upload the custom script file to SA1 - (So the newly modified file is found in sa1).
D- Modify the Custom Script extension Settings on VMSS1 -(This loads the app with the new modifications to some VMs in the VMSS1).
A- Modify the load balancer settings of VMSS1 - (This gets x% of clients to old app y% to newly modified app)

upvoted 11 times

Question #15 *Topic 2*

SIMULATION -
You need to create a notification if the peak average response time of an Azure web app named az400-123456789-main is more than five seconds when evaluated during a five-minute period. The notification must trigger the `https://contoso.com/notify` webhook.
To complete this task, sign in to the Microsoft Azure portal.

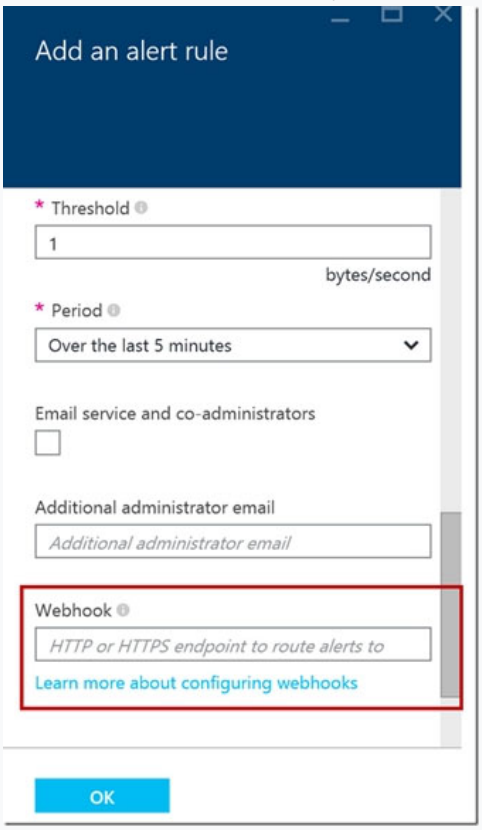
Suggested Answer: *See explanation below.*
1. Open Microsoft Azure Portal
2. Log into your Azure account and go to App Service and look under Monitoring then you will see Alert.
3. Select Add an alert rule
4. Configure the alert rule as per below and click Ok.

Source: Alert on Metrics -
Resource Group: az400-123456789-main

Resource: az400-123456789-main -

Threshold: 5 -

Period: Over the last 5 minutes -
Webhook: https://contoso.com/notify



Reference:
https://azure.microsoft.com/es-es/blog/webhooks-for-azure-alerts/

ozbonny Highly Voted 6 months, 4 weeks ago
In 2024 the steps has changed
but you can follow
go to the web app
go to metrics
got to alerts
go to create/create new rule
select response time
select static

select operator greater than
set threshold 5
next an create an action group or select an existing one that send the notification to the webhook, if you create a new action group just select the action you need in this case webhook and set the url review and create and the keep going with the alert configuration.
upvoted 10 times

renzoku Highly Voted 1 year, 2 months ago
App Services > Web App
Monitoring > Alerts > New alert rule (Resource, Condition, Aggregation type, Time window)
Actions > Add action grohttps://www.examtopics.com/exams/microsoft/az-400/view/5/#up (Action name, Action type, Webhook URI)
upvoted 5 times

chakanirban Most Recent 2 months, 3 weeks ago
NO LAB on 6/21 - 9 am IST -
1 Case study , 6 new Q

1 YES NO series was new - 3 Q - I answered all No , because 2 will No and 1 Y
JOB A depends JOB B
JOB B on JOB C
JOB C on JOB D

who is dependent , who can run parallel
3 yes/ no
upvoted 2 times

rejisundar 1 year, 7 months ago
Webhook need to be created with action group. please refer below link.

https://medium.com/c-sharp-progarmming/azure-alerts-define-alert-rule-in-your-application-service-to-catch-failed-requests-by-webhook-ad987bda1188
upvoted 2 times

Govcomm 2 years, 1 month ago
Azure web app --> Webhook --> Input the URL
upvoted 1 times

dupakonia 2 years, 4 months ago
I think the webhook need to be created in action group and not directly under alert as in the answer
upvoted 5 times

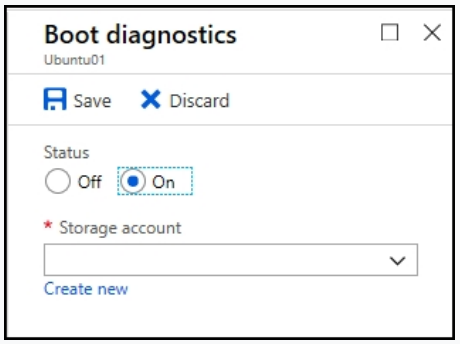
testing 2 years ago
I think that is correct as per below,

https://www.dynatrace.com/support/help/shortlink/azure-alerts#configure-azure-alerts-via-webhook
upvoted 6 times

Question #16 *Topic 2*

SIMULATION -
You need to create and configure an Azure Storage account named az400lod123456789stor in a resource group named RG1lod123456789 to store the boot diagnostics for a virtual machine named VM1.
To complete this task, sign in to the Microsoft Azure portal.

Suggested Answer: *See explanation below.*
Step 1: To create a general-purpose v2 storage account in the Azure portal, follow these steps:
1. On the Azure portal menu, select All services. In the list of resources, type Storage Accounts. As you begin typing, the list filters based on your input. Select
Storage Accounts.
2. On the Storage Accounts window that appears, choose Add.
3. Select the subscription in which to create the storage account.
4. Under the Resource group field, select RG1lod123456789
5. Next, enter a name for your storage account named: az400lod123456789stor
6. Select Create.
Step 2: Enable boot diagnostics on existing virtual machine
To enable Boot diagnostics on an existing virtual machine, follow these steps:
1. Sign in to the Azure portal, and then select the virtual machine VM1.
2. In the Support + troubleshooting section, select Boot diagnostics, then select the Settings tab.
3. In Boot diagnostics settings, change the status to On, and from the Storage account drop-down list, select the storage account az400lod123456789stor.
4. Save the change.



You must restart the virtual machine for the change to take effect.
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-account-create https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/boot-diagnostics

Ranzzzan Highly Voted 1 year, 6 months ago
Under Help section > select boot diagnostics > under setting tab select "Enable with custom storage account" > select storage account and save
upvoted 8 times

chmadhu Most Recent 10 months ago
Does this kind of simulation questions appearing in actual exam?
upvoted 2 times

yana_b 1 year, 1 month ago
Dependent on whether the VM is created or not we have 2 main paths:
1. Create a storage account
2. Go to VM -> Help> Boot diagnostics -> Settings -> "Enable with custom storage account"
2.1. If we have to create the VM -> tab monitoring -> boot diagnostics -> enable with custom storage account and select the storage created in step 1 or, if you first create the VM -> chose create new and create the storage account directly with the creation of the VM
upvoted 2 times

Kent_020 1 year, 2 months ago
What can we see in the real exam for this question? Is it an operation we need to do or we need to choose from some of the options?
upvoted 1 times

AymanAkk 1 year ago

you have an azure portal simulator and you need to do all the steps

upvoted 2 times

Raimyzzz 1 year, 9 months ago

Solution is correct.

upvoted 1 times

emijawdo 1 year, 6 months ago

What solution ? Are you a bot ?

upvoted 1 times

DiligentAmoeba 1 year, 1 month ago

I think he meant the default solution under "Reveal Solution"

upvoted 1 times

SIMULATION -

You have a web app that connects to an Azure SQL Database named db1.

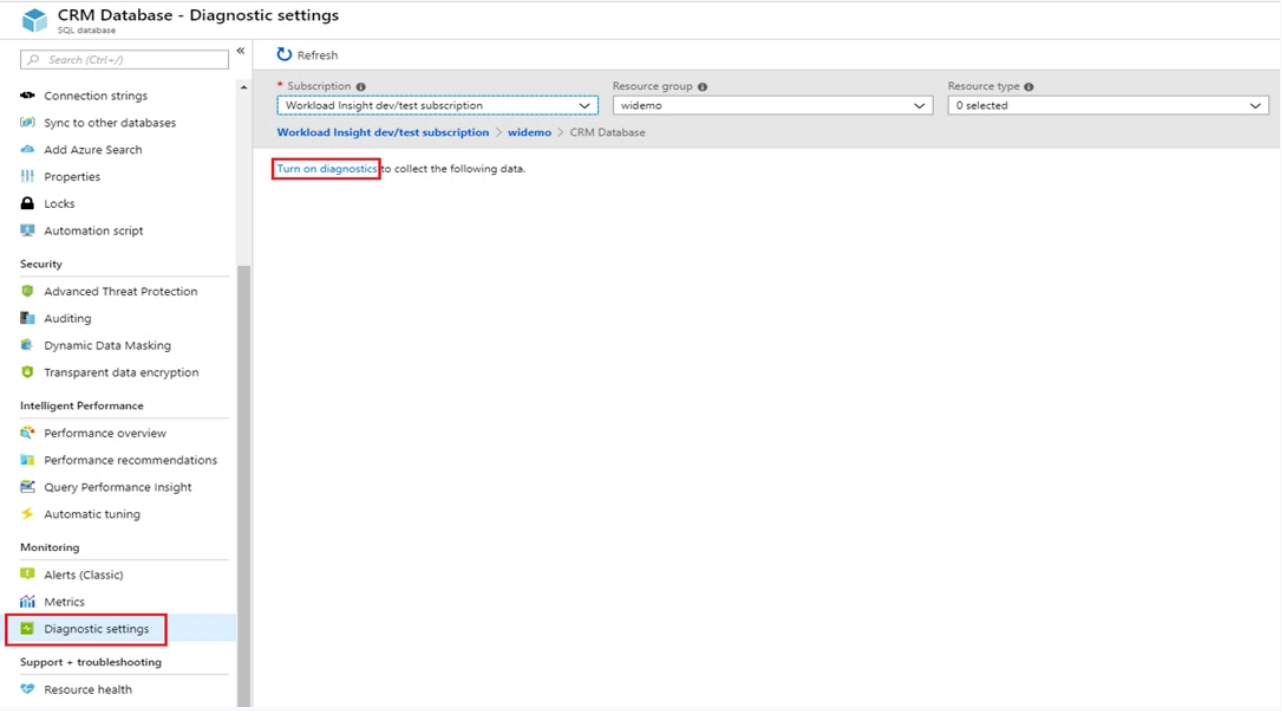
You need to configure db1 to send Query Store runtime statistics to Azure Log Analytics.

To complete this task, sign in to the Microsoft Azure portal.

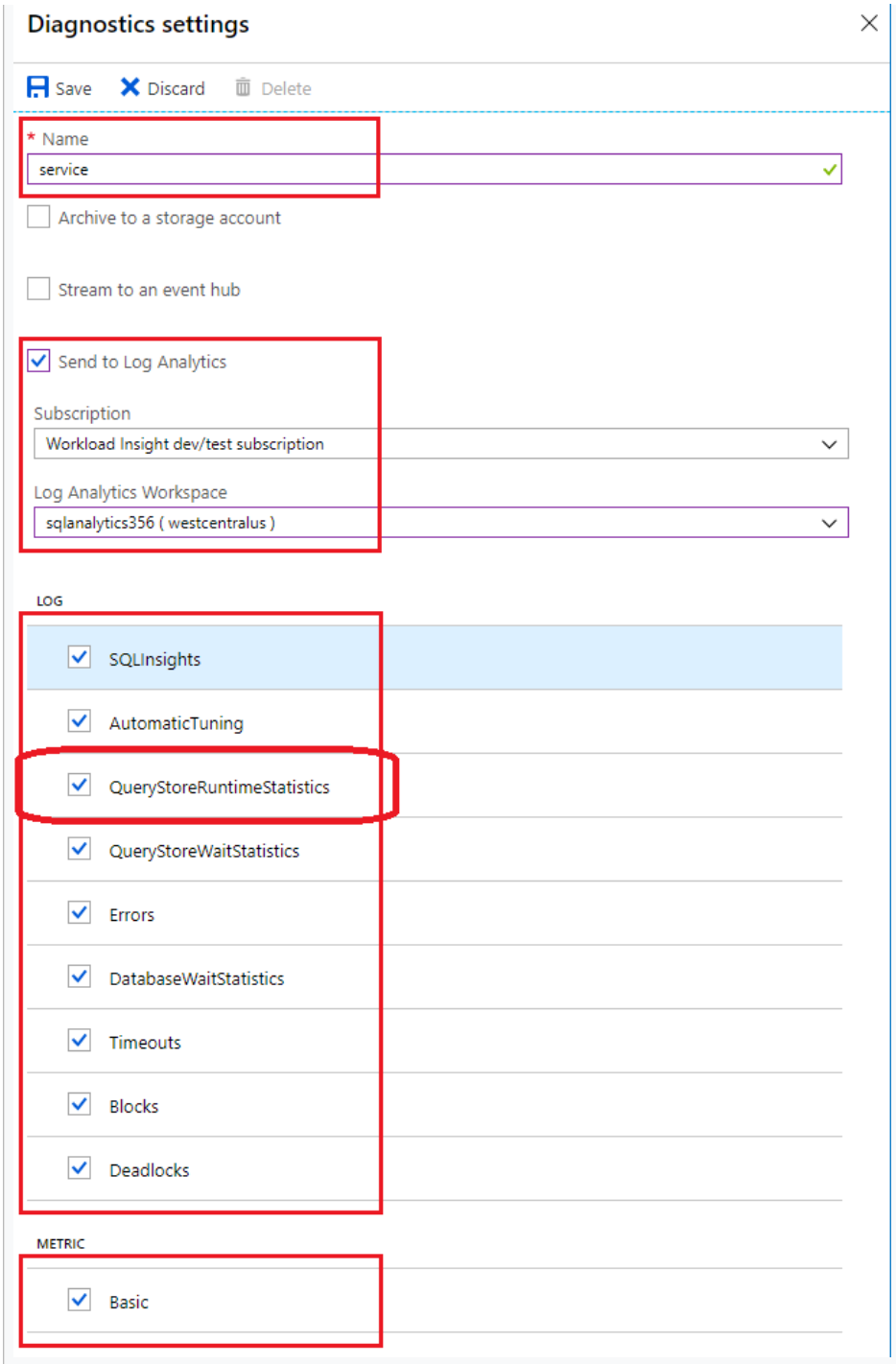
Suggested Answer: *See explanation below.*

To enable streaming of diagnostic telemetry for a single or a pooled database, follow these steps:

1. Go to Azure SQL database resource.
2. Select Diagnostics settings.
3. Select Turn on diagnostics if no previous settings exist, or select Edit setting to edit a previous setting. You can create up to three parallel connections to stream diagnostic telemetry.
4. Select Add diagnostic setting to configure parallel streaming of diagnostics data to multiple resources.



5. Enter a setting name for your own reference.
6. Select a destination resource for the streaming diagnostics data: Archive to storage account, Stream to an event hub, or Send to Log Analytics.
7. For the standard, event-based monitoring experience, select the following check boxes for database diagnostics log telemetry: QueryStoreRuntimeStatistics



8. For an advanced, one-minute-based monitoring experience, select the check box for Basic metrics.
9. Select Save.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/metrics-diagnostic-telemetry-logging-streaming-export-configure

STH Highly Voted 2 years, 6 months ago
there is no more labs in exam, so question is deprecated
upvoted 8 times

ciscogeek 1 year, 4 months ago
Is this true?
upvoted 3 times

deltarj 2 years, 5 months ago
not sure if you're correct. Examtopics Members comment on AZ-400 general discussion differently.. see:
https://www.examtopics.com/exams/microsoft/az-400/
upvoted 4 times

Geraldod 11 months, 3 weeks ago
I wrote 22/09/2023. Had labs

upvoted 3 times

yana_b Highly Voted 1 year, 1 month ago

Provided simulation step-by-step guidance is correct.
I reproduced it in my subscription:
1.Log in to AZ portal and navigate to the AZ SQL database
2. All resources and make sure that there is a Log Analytics Workspace, if no => create one
3. Under Monitoring -> Diagnosstic settings
4. + Add diagnostic setting
5. Give the diagnostic setting a name
6. Check Query Store Runtime Statistics
7. Check basic
8. Check Send to Log Analytics workspace and select the Log Analytics Workspace (if now space exists, you have to 1 create new one and return back here, as no option to creaet one directly from this step)
9. Save

upvoted 6 times

phantom31 3 months, 4 weeks ago

did you create a database first here. you mention nothing about database or querystore here.

upvoted 1 times

peekingpicker 11 months, 4 weeks ago

what happened if we didn't check "basic" in no 7 ?
why must "basic"? how about "InstanceAndAppAdvanced" and "WorkloadManagement" ?

upvoted 2 times

chakanirban Most Recent 2 months, 3 weeks ago

NO LAB on 6/21 - 9 am IST -
1 Case study , 6 new Q

1 YES NO series was new - 3 Q - I answered all No , because 2 will No and 1 Y
JOB A depends JOB B
JOB B on JOB C
JOB C on JOB D

who is dependent , who can run parallel
3 yes/ no

upvoted 3 times

renzoku 1 year, 2 months ago

1. Sign in to the Azure portal
2. Select the Azure SQL Database
3. Configure Log Analytics integration > Diagnostic Settings
4. Enable Query Store data collection

Right?

upvoted 1 times

Govcomm 2 years, 1 month ago

DB --> Diagnostic settings

upvoted 1 times

rdemontis 2 years, 5 months ago

correct answer

upvoted 1 times

apek88 2 years, 12 months ago

Configure this from the Diagnostic settings of the SQL database
https://docs.microsoft.com/en-us/azure/azure-sql/database/metrics-diagnostic-telemetry-logging-streaming-export-configure?tabs=azure-portal#configure-the-streaming-export-of-diagnostic-telemetry

upvoted 3 times

bimbokeem 3 years, 1 month ago

https://docs.microsoft.com/en-us/azure/azure-sql/database/metrics-diagnostic-telemetry-logging-streaming-export-configure?tabs=azure-portal

upvoted 2 times

k8smaster 3 years, 2 months ago

The question asks only for Query Store runtime statistics. Why would you select other options?

upvoted 5 times

STH 2 years, 6 months ago

no need but the exam does not blame you if you do

upvoted 2 times

ham56141 1 year, 8 months ago

Yeah, because Microsoft make more money if you do :)

upvoted 4 times

Question #18 *Topic 2*

DRAG DROP -

You have several Azure virtual machines that run Windows Server 2019.

You need to identify the distinct event IDs of each virtual machine as shown in the following table.

Name	Event ID
VM1	[704, 701, 1501, 1500, 1085]
VM2	[326, 105, 302, 301, 300, 102]
...	...

How should you complete the Azure Monitor query? To answer, drag the appropriate values to the correct locations. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Values

- count()
- makelist(EventID)
- makeset(EventID)
- mv-expand
- project
- render
- summarize

Answer Area

```
Event
| where TimeGenerated > ago(12h)
| order by TimeGenerated desc
| [ ] [ ] by Computer
```

Suggested Answer:

Values

- count()
- makelist(EventID)
- makeset(EventID)
- mv-expand
- project
- render
- summarize

Answer Area

```
Event
| where TimeGenerated > ago(12h)
| order by TimeGenerated desc
| summarize makelist(EventID) by Computer
```

You can use makelist to pivot data by the order of values in a particular column. For example, you may want to explore the most common order events take place on your machines. You can essentially pivot the data by the order of EventIDs on each machine.

Example:

Event -

| where TimeGenerated > ago(12h)

| order by TimeGenerated desc

| summarize makelist(EventID) by Computer

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/advanced-aggregations

an26 Highly Voted 3 years, 5 months ago

You might find it useful to create a list only of distinct values. This list is called a set, and you can generate it by using the makeset command:

Event

| where TimeGenerated > ago(12h)

| order by TimeGenerated desc

| summarize makeset(EventID) by Computer

upvoted 96 times

monniq 3 years, 4 months ago

makeset looks like best option
https://docs.microsoft.com/fi-fi/azure/data-explorer/kusto/query/samples?pivots=azuremonitor
upvoted 6 times

Albelev 3 years, 4 months ago
Event
where TimeGenerated > ago(12h)
order by TimeGenerated desc
summarize makelist(EventID) by Computer

https://docs.microsoft.com/fi-fi/azure/data-explorer/kusto/query/samples?pivots=azuremonitor
upvoted 5 times

AlMargoi 2 years, 9 months ago
It is makeset(EventID) because the output contains unique values.
upvoted 4 times

Webpilot 1 year, 2 months ago
It is obviously makeset. What's different about the function is that it returns a set of unique values.
upvoted 1 times

Zonq Highly Voted 3 years, 5 months ago
I think that correct solution is to use summarize makeset(EventId) as makeset select distinct values. In question there is written: "You need to identify the distinct event IDs of each virtual machine as shown in the following table." and I think we cannot assume that eventId won't repeat in multiple logs.
upvoted 27 times

chloaus Most Recent 5 months, 1 week ago
make_set(): Creates a dynamic array of the set of distinct values that expr takes in the group.
make_list(expr [, maxSize]: Creates a dynamic array of all the values of expr in the group.
https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/make-set-aggregation-function
https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/make-list-aggregation-function
upvoted 2 times

ozbonny 6 months, 4 weeks ago
I'll go by summarize makelist
upvoted 1 times

gabo 11 months, 3 weeks ago
In Whizlabs, the same question has the answer as count() instead of make_set()
upvoted 2 times

yana_b 1 year, 1 month ago
Provided solution is correct
upvoted 1 times

Tyler2023 1 year, 1 month ago
So the requirements is "You need to identify the distinct event IDs"
take note the "distinct"

and here is the difference between set and list

List:
A list is an ordered collection of elements, where duplicate values are allowed.
The order of elements matters, and elements can be accessed by their index in the list.
Lists allow duplicate values, so an element can appear multiple times in the same list.

Set:
A set is an unordered collection of distinct elements, meaning each element can occur only once.
The order of elements does not matter in a set.
Sets do not allow duplicate values, so each element can only appear once in the set.

So that answer should be
summarize makeset(EventId) by Computer
upvoted 2 times

wiliammbr 1 year, 2 months ago
summarize and make_set
make_list does not do distinct
upvoted 3 times

Whatsamattr81 1 year, 7 months ago
says 'distinct' ... i'd use makeset
upvoted 2 times

networkmaniac01 1 year, 7 months ago
Both queries will return distinct event IDs for each virtual machine, but the way the event IDs are presented is different.

The first query, "Event - | where TimeGenerated > ago(12h) | order by TimeGenerated desc | summarize makeset(EventID) by Computer" will return a set of distinct event IDs for each virtual machine, so it will eliminate the duplicate event IDs and will present the event IDs in an unordered format.

The second query, "Event - | where TimeGenerated > ago(12h) | order by TimeGenerated desc | summarize makelist(EventID) by Computer" will return a list of all the event IDs for each virtual machine, including duplicates and will present the event IDs in an ordered format.

So, it depends on the use case, if you want to identify the distinct events and eliminate the duplicates, it is better to use the first query. If you want to see all the events including the duplicates, it's better to use the second query.
upvoted 4 times

xRiot007 1 year, 1 month ago
Only makeset will filter duplicates and return distinct values. The problem states that you need to identify distinct value. Because there are no other operations after the boxes, the only correct option is to use makeset.
upvoted 1 times

srine69 1 year, 12 months ago
make_set() (aggregation function)
Creates a dynamic JSON array of the set of distinct values that Expr takes in the group.

https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/makeset-aggfunction
upvoted 1 times

srine69 1 year, 12 months ago
makelist() has been deprecated in favor of make_list. The legacy version has a default MaxSize limit of 128.
upvoted 2 times

syu31svc 2 years, 1 month ago
https://docs.microsoft.com/fi-fi/azure/data-explorer/kusto/query/samples?pivots=azuremonitor

answer is summarize makeset()
upvoted 3 times

Govcomm 2 years, 1 month ago
summary --> Makelist
upvoted 1 times

Leandrocei 2 years, 2 months ago
Summarize / makeset(EventId). Came today 22 july 9
upvoted 4 times

Eltooth 2 years, 3 months ago
Summarise
Makeset
upvoted 2 times

UnknowMan 2 years, 4 months ago
summarize + makeset (for distinct)
https://docs.microsoft.com/fr-fr/azure/data-explorer/kusto/query/makeset-aggfunction

upvoted 1 times

Question #19 *Topic 2*

HOTSPOT -

You have an Azure web app named Webapp1.

You need to use an Azure Monitor query to create a report that details the top 10 pages of Webapp1 that failed.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
[ exceptions | pageViews | requests | traces ]
| where [ duration == 0 | itemType == "availabilityResult" | resultCode == "200" | success == false ]
| summarize failedCount=sum(itemCount) by name, resultCode
| top 10 by failedCount desc
| render barchart
```

Suggested Answer:

Answer Area

```
[ exceptions | pageViews | requests | traces ]
| where [ duration == 0 | itemType == "availabilityResult" | resultCode == "200" | success == false ]
| summarize failedCount=sum(itemCount) by name, resultCode
| top 10 by failedCount desc
| render barchart
```

Box 1: requests -

Failed requests (requests/failed):

The count of tracked server requests that were marked as failed.

Kusto code:

requests

| where success == 'False'

Box 2: success == false -

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/app-insights-metrics

ScreamingHand Highly Voted 3 years, 2 months ago

Answer looks good to me https://docs.microsoft.com/en-us/azure/azure-monitor/platform/app-insights-metrics

upvoted 23 times

rdemontis 2 years, 6 months ago

you are right!

upvoted 2 times

budha Highly Voted 1 year, 9 months ago

It was on my exam on December 7, 2022.
upvoted 10 times

husam421 Most Recent 2 months, 1 week ago
requests
| where success == 'False'
| summarize sum(itemCount) by bin(timestamp, 5m)
| render barchart
upvoted 2 times

yana_b 1 year, 1 month ago
Provided answer is correct -> for evidence refer to Title: Failed requests (requests/failed) on this page -> https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/app-insights-metrics
upvoted 2 times

MrKingpin 1 year, 6 months ago
Answer is Correct
https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/app-insights-metrics#failed-requests-requestsfailed
upvoted 3 times

GokhanSenyuz 1 year, 10 months ago
Answer is Correct

requests
| where success == 'False'
| summarize sum(itemCount) by bin(timestamp, 5m)
| render barchart

https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/app-insights-metrics
upvoted 4 times

syu31svc 2 years, 1 month ago
Given answer is correct and link provided supports it
upvoted 2 times

Govcomm 2 years, 1 month ago
request --> success == false
upvoted 1 times

UnknowMan 2 years, 4 months ago
Correct (pageviews dont have success or resultcode to query)
upvoted 2 times

Cheehp 2 years, 5 months ago
Selected during exam. requests and success==false.
upvoted 2 times

Axz 2 years, 6 months ago
Got this question today March 2022
upvoted 2 times

RajatSahani 2 years, 9 months ago
given answer is correct
upvoted 2 times

rajvelm 2 years, 10 months ago
Came in today 5th Nov 2021
upvoted 1 times

AZ5cert 3 years ago
Correct Answer: requests and success == 'False'
requests
| where success == 'False'
| summarize sum(itemCount) by bin(timestamp, 5m)
| render barchart

https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/app-insights-metrics

upvoted 3 times

celciuz 3 years ago

This question came out, August 2021

upvoted 2 times

sheva370 3 years, 1 month ago

Tested in my lab. The given answer is correct.

upvoted 1 times

goatlord 3 years, 1 month ago

Seems correct to me after doing Microsoft Learn

upvoted 1 times

Question #20 *Topic 2*

You are monitoring the health and performance of an Azure web app by using Azure Application Insights.
You need to ensure that an alert is sent when the web app has a sudden rise in performance issues and failures.
What should you use?

A. custom events

B. Application Insights Profiler

C. usage analysis

D. Smart Detection

E. Continuous export

Suggested Answer: *D*
Smart Detection automatically warns you of potential performance problems and failure anomalies in your web application. It performs proactive analysis of the telemetry that your app sends to Application Insights. If there is a sudden rise in failure rates, or abnormal patterns in client or server performance, you get an alert.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/proactive-diagnostics

Community vote distribution

D (100%)

davidy2020 Highly Voted 3 years, 2 months ago
Smart detection automatically warns you of potential performance problems and failure anomalies in your web application. It performs proactive analysis of the telemetry that your app sends to Application Insights. If there is a sudden rise in failure rates, or abnormal patterns in client or server performance, you get an alert. This feature needs no configuration. It operates if your application sends enough telemetry.
upvoted 13 times

SteveChai Highly Voted 3 years, 6 months ago
given answer is correct
upvoted 11 times

yana_b Most Recent 1 year, 1 month ago
Selected Answer: D
Smart Detection is correct
upvoted 1 times

Matharax 1 year, 11 months ago
Selected Answer: D
Smart detection. Smart detecetion is bound to Application Insights.
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: D
D is correct as supported by given link
upvoted 1 times

Govcomm 2 years, 1 month ago
Application insights Smart Detection.
upvoted 1 times

Eltooth 2 years, 3 months ago
Selected Answer: D
D is correct answer.
upvoted 1 times

UnknowMan 2 years, 4 months ago
Correct D. Smart Detection
upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: D

correct

https://docs.microsoft.com/en-us/azure/azure-monitor/app/proactive-diagnostics

upvoted 3 times

shermin1 2 years, 6 months ago

Came in exam march 13....

upvoted 1 times

durel 2 years, 7 months ago

On test feb 22

upvoted 2 times

lugospod 2 years, 7 months ago

Got this January 2022

upvoted 2 times

swapmaverick 2 years, 8 months ago

Selected Answer: D

Answer is SmartDetection!!!

upvoted 3 times

RajatSahani 2 years, 9 months ago

given answer is correct

upvoted 1 times

AZ5cert 3 years ago

A: Smart detection

Smart detection detects and notifies about various issues, such as:

Smart detection - Failure Anomalies. We use machine learning to set the expected rate of failed requests for your app, correlating with load, and other factors. Notifies if the failure rate goes outside the expected envelope.

Smart detection - Performance Anomalies. Notifies if response time of an operation or dependency duration is slowing down, compared to historical baseline. It also notifies if we identify an anomalous pattern in response time, or page load time.

General degradations and issues, like Trace degradation, Memory leak, Abnormal rise in Exception volume and Security anti-patterns.

https://docs.microsoft.com/en-us/azure/azure-monitor/app/proactive-diagnostics

upvoted 3 times

goatlord 3 years, 1 month ago

Correct!

upvoted 3 times

Question #21 *Topic 2*

HOTSPOT -

You have a project in Azure DevOps named Contoso App that contains pipelines in Azure Pipelines for GitHub repositories.

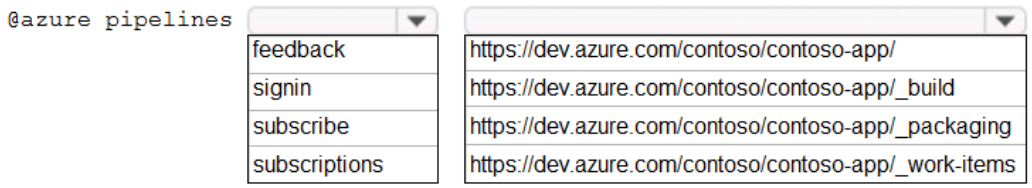
You need to ensure that developers receive Microsoft Teams notifications when there are failures in a pipeline of Contoso App.

What should you run in Teams? To answer, select the appropriate options in the answer area.

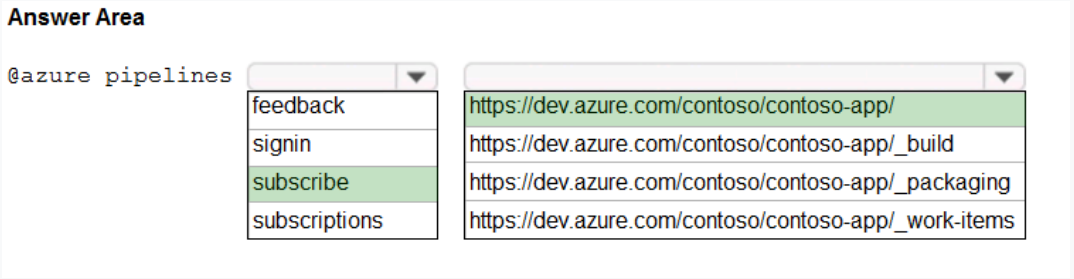
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Suggested Answer:



Box 1: subscribe -

To start monitoring all pipelines in a project, use the following command inside a channel:

@azure pipelines subscribe [project url]

Box 2: https://dev.azure.com/contoso/contoso-app/

Subscribe to a pipeline or all pipelines in a project to receive notifications:

@azure pipelines subscribe [pipeline url/ project url]

haxaffee Highly Voted 3 years, 4 months ago

Given answer is correct: https://docs.microsoft.com/en-us/azure/devops/pipelines/integrations/microsoft-teams?view=azure-devops#connect-the-azure-pipelines-app-to-your-pipelines

@azure pipelines subscribe [project url]

upvoted 48 times

rdemontis 2 years, 5 months ago

agree with you

upvoted 1 times

TrangNguyen_6 2 years, 11 months ago

You are correct!

upvoted 4 times

nvnrao57 Highly Voted 3 years, 4 months ago

Subscribe

https://dev.azure.com/myorg/myproject/_build

upvoted 17 times

Tyler2023 1 year, 1 month ago

The url with _build should have definitionId according to this

https://learn.microsoft.com/en-us/azure/devops/pipelines/integrations/microsoft-teams?view=azure-devops#connect-the-azure-pipelines-app-to-your-pipelines

so that answer is correct

@azure pipelines subscribe https://dev.azure.com/myorg/myproject/

upvoted 4 times

yana_b Most Recent 1 year, 1 month ago
Provided answer is correct
upvoted 3 times

Marge_Simpson 1 year, 7 months ago
@haxaffee The question brings up "a pipeline" instead of all the pipelines. According to the doc you provided:

"Monitor a specific pipeline: The pipeline URL can be to any page within your pipeline that has a definitionId or buildId/releaseId present in the URL. For example, @azure pipelines subscribe https://dev.azure.com/myorg/myproject/_build?definitionId=123."

So

@azure pipelines subscribe [pipeline url]

not the project URL which would monitor all pipelines instead of a pipeline failure
upvoted 3 times

budha 1 year, 9 months ago
It was on my exam on December 7, 2022.
upvoted 3 times

pkg007 2 years ago
Given answer is correct.
Monitor all pipelines in a project " @azure pipelines subscribe [project url] "
Monitor a specific pipeline: "@azure pipelines subscribe [pipeline url]"
upvoted 4 times

syu31svc 2 years, 1 month ago
https://docs.microsoft.com/en-us/azure/devops/pipelines/integrations/microsoft-teams?view=azure-devops#connect-the-azure-pipelines-app-to-your-pipelines

Given answer is correct
upvoted 1 times

Govcomm 2 years, 1 month ago
@azure pipelines subscribe [project url]
upvoted 1 times

Leandrocei 2 years, 2 months ago
Correct. Came today 22 july 9
upvoted 2 times

UnknowMan 2 years, 4 months ago
subscribe https://dev.azure.com/myorg/myproject/_build?definitionId=123 is only for a SPECIFIC pipeline, but here we want all pipeline alert

Correct
upvoted 1 times

Cheehp 2 years, 5 months ago
selected during exam. subscribe and https://dev.azure.com/contoso/contoso-app/
upvoted 1 times

somenkr 2 years, 5 months ago
Given answer is correct
upvoted 1 times

Optimist_Indian 2 years, 7 months ago
Got this question in Feb-2022 exam (scored 910+). Given answer is correct.
upvoted 5 times

ixl2pass 2 years, 9 months ago
Correct. @azure pipelines subscribe https://dev.azure.com/myorg/myproject/ from https://docs.microsoft.com/en-us/azure/devops/pipelines/integrations/microsoft-teams?view=azure-devops

upvoted 1 times

vgr7777 2 years, 9 months ago

@azure pipelines subscribe [project url]

upvoted 1 times

Stark_tony42 2 years, 9 months ago

Wrong

Box1: subscribe

Box2: https://dev.azure.com/whizlabsorg/whizlabs/_build?definitionId=123

upvoted 3 times

ScreamingHand 2 years, 10 months ago

Came in today 5th Nov 2021

upvoted 2 times

Question #22 *Topic 2*

You have a private GitHub repository.
You need to display the commit status of the repository on Azure Boards.
What should you do first?

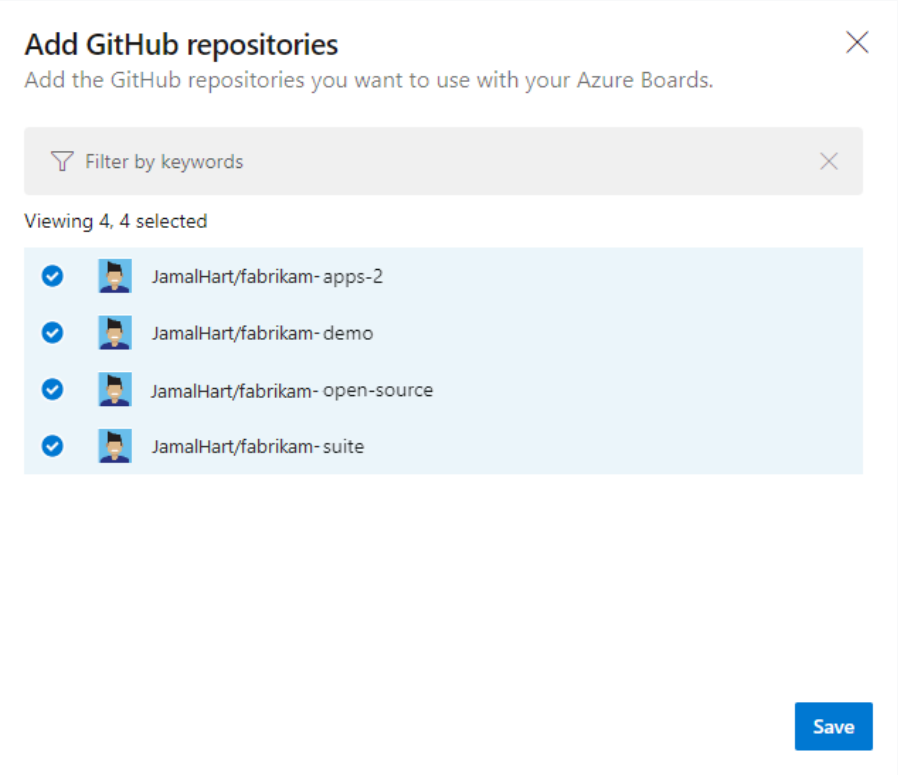
A. Configure multi-factor authentication (MFA) for your GitHub account.

B. Add the Azure Pipelines app to the GitHub repository.

C. Add the Azure Boards app to the repository.

D. Create a GitHub action in GitHub.

Suggested Answer: *C*
To connect Azure Boards to GitHub.com, connect and configure from Azure Boards. Or, alternatively, install and configure the Azure Boards app from GitHub.
Both methods have been streamlined and support authenticating and operating via the app rather than an individual.
Note (see step 4 below):
Add a GitHub connection:
1. Sign into Azure Boards.
2. Choose (1) Project Settings, choose (2) GitHub connections and then (3) Connect your GitHub account.
3. If this is your first time connecting to GitHub from Azure Boards, you will be asked to sign in using your GitHub credentials. Choose an account for which you are an administrator for the repositories you want to connect to.
4. The Add GitHub Repositories dialog automatically displays and selects all GitHub.com repositories for which you are an administrator. Unselect any repositories that you don't want to participate in the integration.



Reference:
https://docs.microsoft.com/en-us/azure/devops/boards/github/connect-to-github

Community vote distribution
C (100%)

ZodiaC Highly Voted 3 years, 2 months ago
Correct:
You will get the results:
https://docs.microsoft.com/en-us/azure/devops/boards/github/install-github-app?view=azure-devops
upvoted 17 times

Sant25 2 years, 11 months ago
CORRECT
upvoted 3 times

Dats1987 Most Recent 12 months ago
Here's why this is the correct choice: B

The Azure Pipelines app is responsible for integrating Azure Pipelines (Azure DevOps CI/CD) with your GitHub repository. By adding this app to your repository, you enable the integration between Azure DevOps (Azure Boards is a part of Azure DevOps) and GitHub.

This integration allows you to automatically trigger builds and release pipelines in Azure Pipelines based on commits, pull requests, or other events in your GitHub repository.

It also enables the communication of commit status and build results from Azure Pipelines to Azure Boards, so you can track the status of your work items (such as user stories or tasks) in Azure Boards based on the build and deployment status in Azure Pipelines.

So, by adding the Azure Pipelines app to your GitHub repository, you establish the link between GitHub and Azure DevOps (which includes Azure Boards), enabling commit status to be displayed in Azure Boards.
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: C
Correct
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: C
Цоррецт
upvoted 1 times

renzoku 1 year, 2 months ago
Selected Answer: C
To do first, establish a connection between GitHub repository and Azure boards
upvoted 2 times

syu31svc 2 years, 1 month ago
Selected Answer: C
C is correct as supported by explanation given
upvoted 1 times

Govcomm 2 years, 1 month ago
Azure board apps for the commit status
upvoted 1 times

Eltooth 2 years, 3 months ago
Selected Answer: C
C is correct answer.
upvoted 1 times

UnknowMan 2 years, 4 months ago
Selected Answer: C
Correct
upvoted 1 times

rdemontis 2 years, 6 months ago
Selected Answer: C
correct
upvoted 1 times

Axz 2 years, 6 months ago
Got this question today March 2022
upvoted 3 times

Whirly 2 years, 6 months ago

Hi Axz, thanks for commenting on Questions appeared in exam, please do add more.
Thanks
upvoted 2 times

gonza89 2 years, 6 months ago

Selected Answer: C

correct answer
upvoted 1 times

gekal 2 years, 11 months ago

Installing the Azure Boards app for GitHub is the first step in connecting Azure Boards to your GitHub repositories.
upvoted 1 times

erico 3 years, 2 months ago

One of the ways to configure Azure Boards and GitHub is to add the Azure Boards Application to the GitHub repository.
upvoted 3 times

igorole 3 years, 2 months ago

All wrong: should be
1. Add a GitHub connection
upvoted 2 times

leonelferrari 3 years, 3 months ago

is Correct!
upvoted 1 times

Question #23 *Topic 2*

You are integrating Azure Pipelines and Microsoft Teams.
You install the Azure Pipelines app in Microsoft Teams.
You have an Azure DevOps organization named Contoso that contains a project name Project1.
You subscribe to Project1 in Microsoft Teams.
You need to ensure that you only receive events about failed builds in Microsoft Teams.
What should you do first?

A. From Microsoft Teams, run @azure pipelines subscribe https://dev.azure.com/Contoso/Project1.

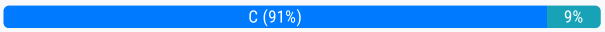
B. From Azure Pipelines, add a Publish Build Artifacts task to Project1.

C. From Microsoft Teams, run @azure pipelines subscriptions.

D. From Azure Pipelines, enable continuous integration for Project1.

Suggested Answer: *A*
To start monitoring all pipelines in a project, use the following command inside a channel:
@azure pipelines subscribe [project url]
The project URL can be to any page within your project (except URLs to pipelines).
For example:
@azure pipelines subscribe https://dev.azure.com/myorg/myproject/
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/integrations/microsoft-teams

Community vote distribution



Appsuri Highly Voted 3 years, 10 months ago
Answer is C
upvoted 60 times

jay158 2 years, 5 months ago
Yes C
https://docs.microsoft.com/en-us/azure/devops/pipelines/integrations/microsoft-teams?view=azure-devops#manage-subscriptions
upvoted 5 times

warchoon 1 year, 9 months ago
No A
Just see section "Use commands"
upvoted 2 times

warchoon 1 year, 9 months ago
Ок C
Missed the filter option. It's bad for teams not to provide the command
upvoted 3 times

babiend20 Highly Voted 3 years, 10 months ago
Answer is C
https://docs.microsoft.com/en-us/azure/devops/pipelines/integrations/microsoft-teams?view=azure-devops
Using filters effectively to customize subscriptions
When a user subscribes to any pipeline, a few subscriptions are created by default without any filters being applied. Often, users have the need to customize these subscriptions. For example, users may want to get notified only when builds fail or when deployments are pushed to a production environment. The Azure Pipelines app supports filters to customize what you see in your channel.

Run the @Azure Pipelines subscriptions command
Select View all subscriptions. In the list of subscriptions, if there is a subscription that is unwanted or should be modified (Example: creating noise in the channel), select Remove
Scroll down and select the Add subscription button

Select the required pipeline and the event
Select the appropriate filters and save
upvoted 30 times

husam421 Most Recent 2 months, 1 week ago
Selected Answer: C
Run the @azure pipelines subscriptions command.
upvoted 2 times

e0da014 3 months, 2 weeks ago
Option C , Refer this: https://learn.microsoft.com/en-us/azure/devops/pipelines/integrations/microsoft-teams?view=azure-devops

Manage subscriptions
When you subscribe to a pipeline, a few subscriptions get created by default without any filters applied. You might want to customize these subscriptions. For example, you might want to get notified only when builds fail or when deployments get pushed to a production environment. The Azure Pipelines app supports filters to customize what you see in your channel. To manage your subscriptions, complete the following steps.

Run the @azure pipelines subscriptions command
upvoted 1 times

Pavlo 4 months, 3 weeks ago
C. From Microsoft Teams, run @azure pipelines subscriptions.

This command allows you to manage your subscriptions within Microsoft Teams, including specifying the types of events you want to receive notifications for, such as failed builds. By running this command, you can set up a subscription specifically for failed build events, ensuring that you only receive notifications relevant to your requirement.
upvoted 1 times

FiedlExamopics 6 months, 1 week ago
The correct answer is A, the link https://learn.microsoft.com/en-us/azure/devops/pipelines/integrations/microsoft-teams?view=azure-devops clearly states that you have to subscribe to a project first of all, before you can modify and make any modifications to the subscription.
If C is done before A, there is no assigned project subscription to the pipeline which would not make sense.
The question asks what needs to be done first and that is A before C.
upvoted 2 times

ozbonny 6 months, 3 weeks ago
Selected Answer: C
C
https://learn.microsoft.com/en-us/azure/devops/pipelines/integrations/microsoft-teams?view=azure-devops
upvoted 1 times

ozbonny 6 months, 4 weeks ago
Selected Answer: C
I think C. From Microsoft Teams, run @azure pipelines subscriptions. since you already subscribed to the project
upvoted 1 times

ozbonny 6 months, 4 weeks ago
Selected Answer: C
I think You subscribe to Project1 in Microsoft Teams. since the first step is already done.
upvoted 1 times

kleansoul 11 months, 4 weeks ago
Selected Answer: C
When you subscribe to a pipeline, a few subscriptions get created by default without any filters applied. You might want to customize these subscriptions. For example, you might want to get notified only when builds fail or when deployments get pushed to a production environment. The Azure Pipelines app supports filters to customize what you see in your channel. To manage your subscriptions, complete the following steps.

Run the @azure pipelines subscriptions command.
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: C
Go to your teams project channel -> type in @azure pipelines and then select subscriptions -> when the list with subscriptions appears on your screen => select view all subscriptions -> under each subscription there is remove button

upvoted 1 times

renzoku 1 year, 2 months ago

Selected Answer: C

1. run @azure pipelines subscriptions
2. select the project "Project1"
3. Set up a subscriptions for failed builds, then you will receive notifications in Teams

upvoted 2 times

KumaTed 1 year, 3 months ago

yeah, the answer is C ,definitely

upvoted 2 times

icedog 1 year, 7 months ago

Selected Answer: C

It's C

From the preamble in the question option A has already been done (You Subscript to Project1 in Microsoft Team"

To ensure you only receive failure events you need to run @azure pipelines subscriptions and from there you can manage filters

upvoted 5 times

AvinashVarma 1 year, 8 months ago

Selected Answer: C

Given requirement: Receive events about failed builds. This can be achieved by runnning "Azure Pipelines subscriptions" in Teams Converstation and click on "Add Subscription" for more filter options like choosing "Build Status: Failed".

The answer is C.

Reference: https://learn.microsoft.com/en-us/azure/devops/pipelines/integrations/microsoft-teams?view=azure-devops#manage-subscriptions

upvoted 2 times

SingularityLady 1 year, 8 months ago

Selected Answer: A

I think A is the correct option because the question is: "What should you do first?"

upvoted 2 times

Amutha_25 1 year, 7 months ago

You have already subscribed to Project1 in Microsoft Teams. Read the question again

upvoted 5 times

rikininetysix 1 year, 8 months ago

Selected Answer: C

Answer seems to be 'C'. Refer to 'Manage Subscription' section of the document - https://github.com/MicrosoftDocs/azure-devops-docs/blob/main/docs/pipelines/integrations/microsoft-teams.md

"For example, you might want to get notified only when builds fail or when deployments get pushed to a production environment. The Azure Pipelines app supports filters to customize what you see in your channel. To manage your subscriptions, complete the following steps.

Run the @azure pipelines subscriptions command."

upvoted 1 times

Question #24 *Topic 2*

You have an Azure DevOps organization named Contoso.
You need to receive Microsoft Teams notifications when work items are updated.
What should you do?

A. From Azure DevOps, configure a service hook subscription

B. From Microsoft Teams, configure a connector

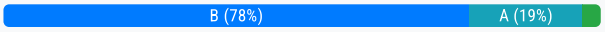
C. From the Microsoft Teams admin center, configure external access

D. From Microsoft Teams, add a channel

E. From Azure DevOps, install an extension

Suggested Answer: *A*
Service hooks let you run tasks on other services when events happen in your Azure DevOps projects. For example, create a card in Trello when a work item is created or send a push notification to your team's mobile devices when a build fails. You can also use service hooks in custom apps and services as a more efficient way to drive activities when events happen in your projects.
Note: Service hook publishers define a set of events. Subscriptions listen for the events and define actions to take based on the event. Subscriptions also target consumers, which are external services that can run their own actions, when an event occurs.
Reference:
https://docs.microsoft.com/en-us/azure/devops/service-hooks/overview

Community vote distribution



SriLen Highly Voted 3 years, 7 months ago
B. From Microsoft Teams, Configure a connector.
if you try from Azure DevOps, you getting the following message:
Subscriptions for this service are managed by the consumer service. To create a new subscription visit Microsoft Teams.

So it is not possible from DevOps Any more, just verified
upvoted 66 times

jay158 2 years, 5 months ago
Why not D
https://docs.microsoft.com/en-us/azure/devops/boards/integrations/boards-teams?view=azure-devops
Can anyone explain please
upvoted 3 times

arr73 4 months, 4 weeks ago
I think it's not D because you can use an existing channel. Not needed to create a new one. Documentation says "You add the app to your Teams channel in Microsoft Teams"
Ref: https://learn.microsoft.com/en-us/azure/devops/boards/integrations/boards-teams?view=azure-devops#add-the-azure-boards-app-to-microsoft-teams
upvoted 1 times

sylviea Highly Voted 3 years, 10 months ago
B. From Microsoft Teams, configure a connector
https://azuredevopslabs.com/labs/vstsextend/teams/
upvoted 24 times

harshit101 Most Recent 3 months, 3 weeks ago
Selected Answer: A
A is correct.
https://learn.microsoft.com/en-us/azure/devops/organizations/notifications/manage-team-group-global-organization-notifications?view=azure-devops
upvoted 2 times

ay_m 3 months, 1 week ago

The question is about integrating Azure DevOps with Microsoft Teams, the link you shared does not tell you how to send notifications to a Teams channel, but to individual project members by email.

This is the correct link:
https://learn.microsoft.com/en-us/azure/devops/boards/integrations/boards-teams?view=azure-devops#add-the-azure-boards-app-to-microsoft-teams
upvoted 1 times

kiko90909 4 months ago
A. From Azure DevOps, configure a service hook subscription

Here is how you can do it:

In your Azure DevOps project, navigate to Project settings.
Under Service hooks, create a new subscription.
Choose Microsoft Teams as the service.
Configure the subscription to trigger on work item updates and specify the details of the Teams channel where you want to send the notifications.
This setup allows Azure DevOps to send notifications to Microsoft Teams based on the conditions you specify (e.g., when a work item is updated).
upvoted 3 times

ozbonny 6 months, 4 weeks ago
Selected Answer: B
I'll go by B due to this doc
https://learn.microsoft.com/en-us/azure/devops/service-hooks/services/teams?view=azure-devops#configure-a-new-connector-for-azure-devops-server
upvoted 1 times

Dimpzz 10 months, 3 weeks ago
B.
The order of steps is B and then A.
https://learn.microsoft.com/en-us/azure/devops/service-hooks/services/teams?view=azure-devops
upvoted 1 times

Dats1987 11 months, 2 weeks ago
A will be the answer:
You can use a connector to connect Microsoft Teams to Azure DevOps, but you still need to configure a service hook subscription in Azure DevOps to receive notifications.

If you read the question carefully. Objective is to receive the notification..
upvoted 1 times

gabo 11 months, 3 weeks ago
To just receive a notification from Azure DevOps, a service hook should be sufficient. Can someone explain why that's not the case?
upvoted 1 times

KayLuv 1 year ago
Selected Answer: A
A is the correct answer.
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: B
Configuring integration between Azure DevOps Server and Teams is a two-step process. First set up a connector in Teams, then set up one or more service hook subscriptions in your Azure DevOps Server project.
https://learn.microsoft.com/en-us/azure/devops/service-hooks/services/teams?view=azure-devops ->
upvoted 4 times

vivekcloud 8 months ago
Correct. First u need to configure connector in Teams from where u will get the webhook url which u can use while setting up the service hook in the Azure devops.
upvoted 1 times

AxiansPT 1 year, 1 month ago

A. https://learn.microsoft.com/en-us/azure/devops/service-hooks/services/teams?view=azure-devops
You first create the service hook from azure devops, second step create the connector in teams.
upvoted 1 times

_alex_123 10 months, 3 weeks ago
Need to swap the order and then your are right:
"Configuring integration between Azure DevOps Server and Teams is a two-step process. First set up a connector in Teams, then set up one or more service hook subscriptions in your Azure DevOps Server project." - https://learn.microsoft.com/en-us/azure/devops/service-hooks/services/teams?view=azure-devops
upvoted 2 times

Vaibhab 1 year, 1 month ago
Answer is A, Service hooks allow you to configure notifications and integrations between Azure DevOps and other external services like Microsoft Teams
upvoted 2 times

renzoku 1 year, 2 months ago
Selected Answer: B
B. From Microsoft Teams, configure a connector
Allow connect with external services, install it in Teams allow to integrate Microsoft Teams with Azure Devops.

A. From Azure DevOps, configure a service hook subscription
Allow react to events within Azure Devops and automate actions in response.
upvoted 1 times

zellck 1 year, 3 months ago
Selected Answer: B
B is the answer.

https://learn.microsoft.com/en-us/azure/devops/service-hooks/services/teams?view=azure-devops#configure-a-new-connector-for-azure-devops-server
Configuring integration between Azure DevOps Server and Teams is a two-step process. First set up a connector in Teams, then set up one or more service hook subscriptions in your Azure DevOps Server project.
upvoted 5 times

ShomaV 1 year, 3 months ago
To integrate Azure DevOps with Microsoft Teams, it is recommended to use a connector rather than a service hook subscription.

Connectors provide a more streamlined and user-friendly integration experience between Azure DevOps and Microsoft Teams.
upvoted 1 times

318touring 1 year, 4 months ago
Selected Answer: B
Option B as when trying to do Opt A, you'd receive this message "Subscriptions for this service are managed by the consumer service. To create a new subscription visit Microsoft Teams."
upvoted 3 times

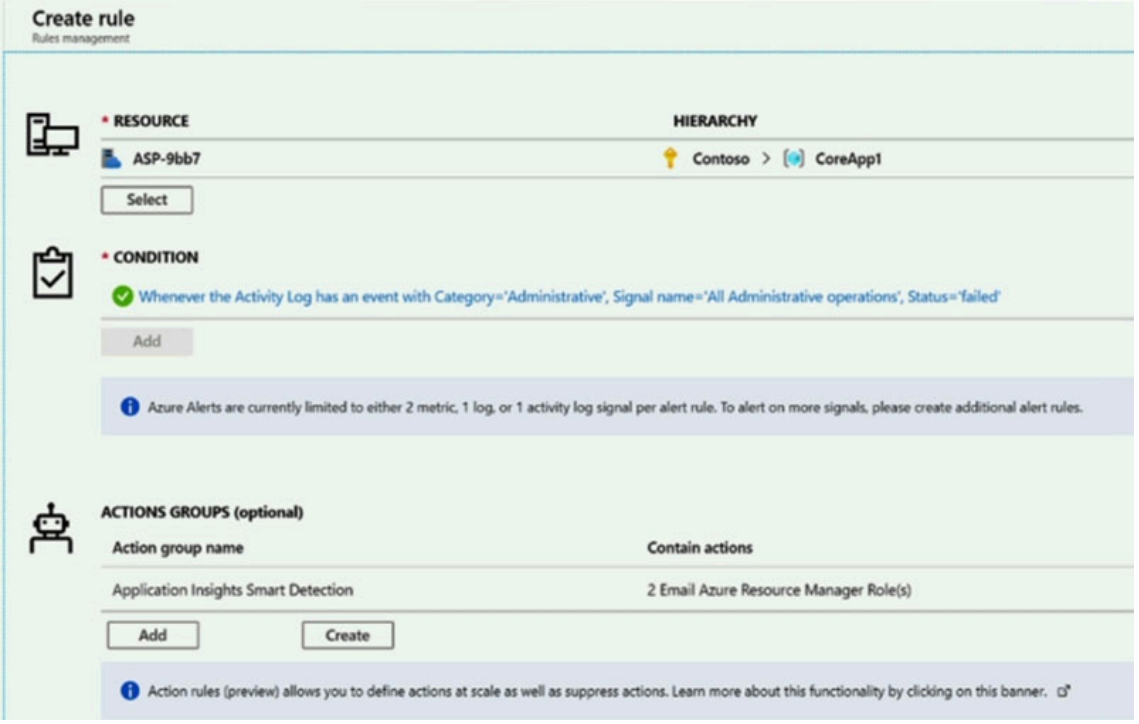
col2511kol 1 year, 5 months ago
Selected Answer: B
While configuring a service hook subscription in Azure DevOps (Option A) is one way to set up notifications for events like work item updates, it doesn't directly send notifications to Microsoft Teams. You would still need to create a custom integration between the service hook and Microsoft Teams to receive notifications, which can be complex and time-consuming.

On the other hand, Option B - configuring a connector in Microsoft Teams - is a more straightforward approach. Microsoft Teams provides a built-in connector for Azure DevOps, which allows you to easily receive notifications for work item updates directly within a Teams channel. This simplifies the setup process, making it a more suitable solution for your requirement.

In summary, while both options could ultimately achieve the desired outcome, configuring a connector in Microsoft Teams (Option B) is a more direct and convenient method for receiving notifications when work items are updated in Azure DevOps.
upvoted 4 times

Question #25 *Topic 2*

You create an alert rule in Azure Monitor as shown in the following exhibit.



Which action will trigger an alert?

A. a failed attempt to delete the ASP-9bb7 resource

B. a change to a role assignment for the ASP-9bb7 resource

C. a successful attempt to delete the ASP-9bb7 resource

D. a failed attempt to scale up the ASP-9bb7 resource

Suggested Answer: *A*

Community vote distribution

A (100%)

Nilf Highly Voted 3 years, 4 months ago

Correct...

Condition - Failed. So it's should be A or D... But Administrative it's Contains the record of all create, update, delete, and action operations performed through Resource Manager.

So answer is A

upvoted 22 times

ozbonny Most Recent 6 months, 4 weeks ago

Selected Answer: A

IMO. A. a failed attempt to delete the ASP-9bb7 resource

upvoted 2 times

yana_b 1 year, 1 month ago

Selected Answer: A

Administrative => all create, delete, update, action operations.

We want the ones that failed.

Answer is A

upvoted 2 times

xRiot007 1 year, 2 months ago

Answer is A.

The alert is triggered on a failure, so B and C are excluded right away.

The D option, scaling, is not an administrative action
The A option, deleting, is an administrative action.
upvoted 2 times

zellck 1 year, 3 months ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log-schema#categories
- Administrative
Contains the record of all create, update, delete, and action operations performed through Resource Manager. Examples of Administrative events include create virtual machine and delete network security group.

Every action taken by a user or application using Resource Manager is modeled as an operation on a particular resource type. If the operation type is Write, Delete, or Action, the records of both the start and success or fail of that operation are recorded in the Administrative category. Administrative events also include any changes to Azure role-based access control in a subscription.
upvoted 4 times

syu31svc 2 years, 1 month ago

Selected Answer: A

Status failed so this rules out B and C

https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log-schema:

"Administrative Contains the record of all create, update, delete, and action operations performed through Resource Manager. Examples of Administrative events include create virtual machine and delete network security group."

A is the answer
upvoted 3 times

Govcomm 2 years, 1 month ago

Category is administrative so it is related to the resource creation, update and deletion.
upvoted 2 times

debleenac85 2 years, 5 months ago

One doubt. The scope of the resource is app service plan. I believe D is the correct answer as if we scale a resource the app service plan gets updated.
upvoted 2 times

debleenac85 2 years, 5 months ago

Sorry pls ignore my comment. This will be A
upvoted 2 times

prashantjoge 2 years, 5 months ago

because d is an autoscale event, not an administrative event
upvoted 3 times

basw77 2 years, 2 months ago

autoscale only does scale-out not scale-up, as mentioned in the answer
upvoted 1 times

basw77 2 years, 2 months ago

I think so too. There is a simular question in the official practice exam. Removal of the resource was a wrong answer. So scale-UP (so not autoscale OUT) is the only option left.
upvoted 3 times

catfood 1 year, 1 month ago

saw that and I'm still confused
upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: A

Correct
https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log-schema

upvoted 3 times

gonza89 2 years, 6 months ago

Selected Answer: A

correct answer

upvoted 1 times

Art3 2 years, 8 months ago

answer A is correcct

upvoted 1 times

AZ5cert 3 years ago

Correct Answer A

Activity log events record stop, start, delete resource.

upvoted 3 times

sheva370 3 years, 1 month ago

Tested in my lab. The given answer is correct.

upvoted 2 times

kovas6 3 years, 5 months ago

is it correct?

upvoted 3 times

vasonic 3 years, 5 months ago

Looking at the conditions, I think it's correct.

upvoted 2 times

Miles19 3 years, 5 months ago

It's correct. https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log-schema

upvoted 3 times

Question #26 *Topic 2*

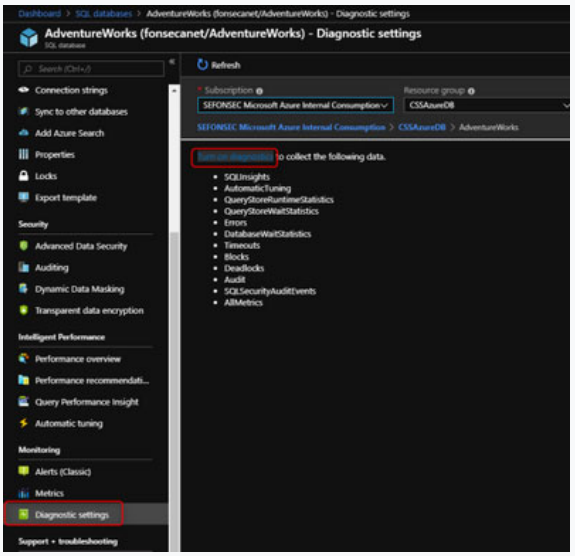
You have a web app hosted on Azure App Service. The web app stores data in an Azure SQL database.
You need to generate an alert when there are 10,000 simultaneous connections to the database. The solution must minimize development effort.
Which option should you select in the Diagnostics settings of the database?

A. Send to Log Analytics

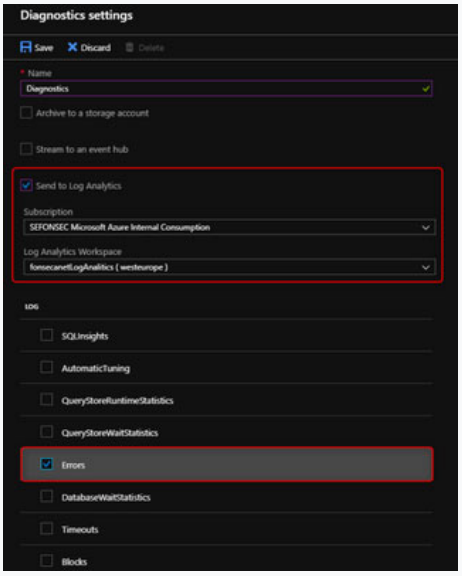
B. Stream to an event hub

C. Archive to a storage account

Suggested Answer: *A*
ENABLE DIAGNOSTICS TO LOG ANALYTICS
This configuration is done PER DATABASE
1. Click on Diagnostics Settings and then Turn On Diagnostics



2. Select to Send to Log Analytics and select the Log Analytics workspace. For this sample I will selected only Errors



Reference:
https://techcommunity.microsoft.com/t5/azure-database-support-blog/azure-sql-db-and-log-analytics-better-together-part-1/ba-p/794833

Community vote distribution

A (100%)

luclasses Highly Voted 3 years, 4 months ago
CorrectJacints
upvoted 14 times

Dalias Highly Voted 3 years, 2 months ago

Got this in 30 June 2021 exam. Scored 800+ the provided answer is correct - A

upvoted 10 times

AymanAkk Most Recent 1 year ago

the other options are werid

upvoted 1 times

yana_b 1 year, 1 month ago

Selected Answer: A

Given answer is correct

upvoted 1 times

mohiniu 1 year, 6 months ago

According to chatgpt answer is eventhub

upvoted 1 times

ABC666 1 year, 8 months ago

Selected Answer: A

Correct!

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: A

100% is A

upvoted 3 times

tjeerd 2 years, 1 month ago

Selected Answer: A

On exam 20220727.

upvoted 1 times

Govcomm 2 years, 1 month ago

Azure log analytics query using KQL

upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct, A to create an alert

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: A

correct. the simplest way to archive data and to generate the alert

upvoted 1 times

Optimist_Indian 2 years, 7 months ago

Got this question in Feb-2022 exam (scored 910+). Given answer is correct. Log Analytics.

upvoted 3 times

subrata83 2 years, 11 months ago

Got this question on 27th sep, 2020, answered A

upvoted 3 times

volturyon 3 years, 4 months ago

correct!

upvoted 8 times

HOTSPOT -

You use Azure DevOps to manage the build and deployment of an app named App1.

You have a release pipeline that deploys a virtual machine named VM1.

You plan to monitor the release pipeline by using Azure Monitor.

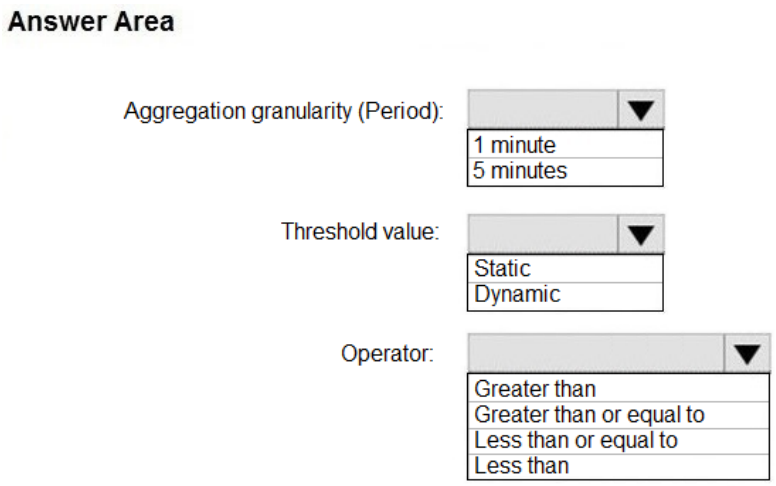
You need to create an alert to monitor the performance of VM1. The alert must be triggered when the average CPU usage exceeds 70 percent for five minutes.

The alert must calculate the average once every minute.

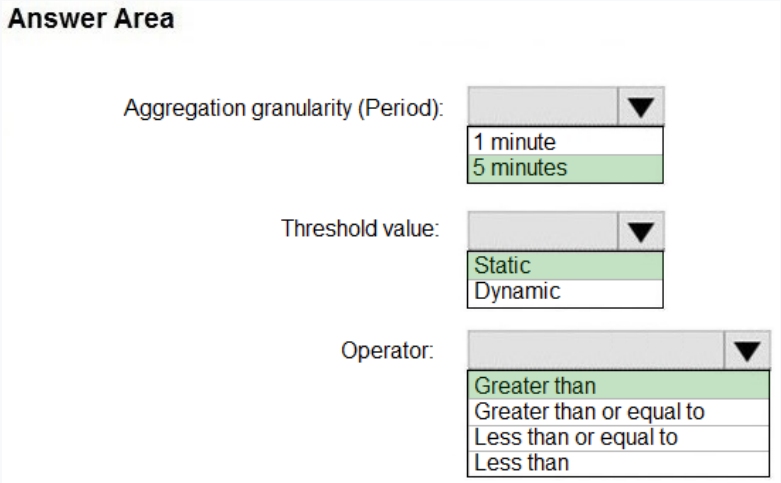
How should you configure the alert rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:



Box 1: 5 minutes -

The alert must calculate the average once every minute.

Note: We [Microsoft] recommend choosing an Aggregation granularity (Period) that is larger than the Frequency of evaluation, to reduce the likelihood of missing the first evaluation of added time series

Box 2: Static -

Box 3: Greater than -

Example, say you have an App Service plan for your website. You want to monitor CPU usage on multiple instances running your web site/app. You can do that using a metric alert rule as follows:

- Target resource: myAppServicePlan
- Metric: Percentage CPU
- Condition Type: Static
- Dimensions
- Instance = InstanceName1, InstanceName2
- Time Aggregation: Average
- Period: Over the last 5 mins

➪ Frequency: 1 min
➪ Operator: GreaterThan
➪ Threshold: 70
➪ Like before, this rule monitors if the average CPU usage for the last 5 minutes exceeds 70%.
➪ Aggregation granularity
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric-overview

JerryGolais Highly Voted 3 years, 3 months ago
Correct answer:
5 Min
Static
Greater than
upvoted 53 times

ukohae39 3 years, 2 months ago
Verified!
upvoted 3 times

vxl 1 year, 7 months ago
Correct, came up in my exam (2023)
upvoted 9 times

rdemontis 2 years, 5 months ago
you are right
upvoted 1 times

nvnrao57 Highly Voted 3 years, 4 months ago
1 Min
Static
Greater than
upvoted 12 times

coffecold 1 year, 10 months ago
Aggregation is 1 minute. "Time granularity or time grain – The time period used to aggregate values together to allow display on a chart. Only specific ranges are available. Current minimum is 1 minute. The time granularity value should be smaller than the selected time range to be useful, otherwise just one value is shown for the entire chart."
https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/metrics-aggregation-explained
upvoted 2 times

BalderkVeit 3 years, 4 months ago
"The alert must be triggered when the average CPU usage exceeds 70 percent for five minutes", so Aggregation granularity (period) is 5 minutes. Frequency would be 1 minute.
Static - agree
greater than - agree

There's exact example in provided documentation.
upvoted 36 times

navinm1 Most Recent 11 months, 4 weeks ago
This question came in my exam on 23-Sep-23. I have selected the given answer and I have passed (Score 844).
upvoted 4 times

EngineTyme 11 months, 3 weeks ago
Did you have labs in your exams?
upvoted 3 times

yana_b 1 year, 1 month ago
Correct answer.
Static due to the fact that it is not based on % from a pattern, but from a hardcoded number.
Greater than as it says above/exceeds and not when CPU reaches 70% or more.
Granularity -> gives the time duration for which we calculate the filter rule (exceeds 70% within time duration of 5 minutes => send alert).
upvoted 2 times

zellck 1 year, 3 months ago
1. 5 minutes
2. Static
3. Greater than

https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-create-new-alert-rule?tabs=metric#create-a-new-alert-rule-in-the-azure-portal
- Aggregation granularity
Select the interval that's used to group the data points by using the aggregation type function. Choose an Aggregation granularity (period) that's greater than the Frequency of evaluation to reduce the likelihood of missing the first evaluation period of an added time series.
upvoted 4 times

zellck 1 year, 3 months ago
Gotten this in Jun 2023 exam.
upvoted 6 times

essay 1 year, 2 months ago
Do you perhaps have contributor access?, are you willing to share your deets with me? @zellck, my email is passioneng74@gmail.com.
upvoted 1 times

AlexeyG 1 year, 6 months ago
got this in 02 March 2023 exams. scored 870 marks.
upvoted 7 times

nikipediaa 1 year, 7 months ago
Got this Feb 2023
upvoted 2 times

syu31svc 2 years, 1 month ago
"The alert must be triggered when the average CPU usage exceeds 70 percent for five minutes."

Given answer is correct
upvoted 4 times

Govcomm 2 years, 1 month ago
Static alert when CPU is greater than 70% for 5 minutes.
upvoted 2 times

UnknowMan 2 years, 4 months ago
Correct
upvoted 1 times

AnshMan 2 years, 4 months ago
https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-metric-overview

5 Min (aggregation types are Minimum, Maximum, Average, Total, Count)
Static and
Greater than

Refer to the above link, if in exam it is frequency instead of Agregation/Period we should select 1 min
upvoted 3 times

Cheehp 2 years, 5 months ago
Selected during exam.
5 Min
Static
Greater than
upvoted 2 times

RajatSahani 2 years, 9 months ago
Given Answer is correct - 5 Min, Static, Greater than
upvoted 1 times

ScreamingHand 2 years, 10 months ago
Came in today 5th Nov 2021

upvoted 1 times

Aniruddha_dravyakar 2 years, 10 months ago

5min

Dynamic

Greater than

upvoted 1 times

d0bermannn 2 years, 12 months ago

5min-static-ge

obvious for az104

upvoted 1 times

goatlord 3 years, 1 month ago

CORRECT

upvoted 1 times

Question #28 *Topic 2*

You have an Azure virtual machine that is monitored by using Azure Monitor.
The virtual machine has the Azure Log Analytics agent installed.
You plan to deploy the Service Map solution from the Azure Marketplace.
What should you deploy to the virtual machine to support the Service Map solution?

A. the Dependency agent

B. the Telegraf agent

C. the Windows Azure diagnostics extension (WAD)

D. the Azure monitor agent

Suggested Answer: *A*
Use the Dependency agent if you need to use the Map feature VM insights or the Service Map solution.
Note: Consider the following when using the Dependency agent:
The Dependency agent requires the Log Analytics agent to be installed on the same machine.
On Linux computers, the Log Analytics agent must be installed before the Azure Diagnostic Extension.
On both the Windows and Linux versions of the Dependency Agent, data collection is done using a user-space service and a kernel driver.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview

Community vote distribution
A (100%)

Matharax Highly Voted 1 year, 11 months ago
Selected Answer: A
Verified, had this on the exam.
upvoted 6 times

CommanderBigMac 1 year ago
Does mean your answer is magically correct
upvoted 4 times

garbas Most Recent 12 months ago
Selected Answer: A
https://learn.microsoft.com/en-us/azure/azure-monitor/vm/vminsights-enable-overview#agents

Log Analytics agent is going to be replaced by Azure Monitor agent
Service Map is going to be replaced by Azure Monitor VM insights
But the Dependency agent is still required
In fact, both agents are automatically installed when Azure Monitor VM insights is enabled
upvoted 2 times

renzoku 1 year, 2 months ago
Selected Answer: A
Azure Service Map. monitoring solution that discovers dependencies between different components of your application, all in an interactive visual representation.

Dependency agent. Specially designed to collect different information between your components, allowing visualize the dependency accurately.
upvoted 3 times

zellck 1 year, 3 months ago
Selected Answer: A
A is the answer.

https://learn.microsoft.com/en-us/azure/azure-monitor/vm/vminsights-dependency-agent-maintenance
The Dependency Agent collects data about processes running on the virtual machine and external process dependencies.
upvoted 3 times

surensaluka 1 year, 7 months ago

Selected Answer: A

This came today for my exam on 2023-02-14. Selected A as the answer.

upvoted 2 times

budha 1 year, 9 months ago

It was on my exam on December 7, 2022.

upvoted 3 times

coffecold 1 year, 10 months ago

"If you have machines already deployed with legacy Log Analytics agents, we recommend you migrate to Azure Monitor Agent as soon as possible. The legacy Log Analytics agent will not be supported after August 2024."

Isn't Azure Monitor Agent replacing all the agents?

upvoted 2 times

coffecold 1 year, 10 months ago

Dependency agent

upvoted 1 times

coffecold 1 year, 10 months ago

https://learn.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview

upvoted 1 times

pkg007 2 years ago

Answer is A

The prerequisites of the Service Map solution are the following:

1. A Log Analytics workspace in a supported region.
2. The Log Analytics agent installed on the Windows computer or Linux server connected to the same workspace that you enabled the solution with.
3. The Dependency agent installed on the Windows computer or Linux server.

upvoted 1 times

syu31svc 2 years ago

Selected Answer: A

https://docs.microsoft.com/en-us/azure/azure-monitor/vm/service-map

"The prerequisites of the solution are the following:

A Log Analytics workspace in a supported region.

The Log Analytics agent installed on the Windows computer or Linux server connected to the same workspace that you enabled the solution with.

The Dependency agent installed on the Windows computer or Linux server."

Answer is A

upvoted 2 times

rinjohn 2 years ago

Selected Answer: A

Correct

https://docs.microsoft.com/en-us/azure/azure-monitor/vm/service-map

upvoted 3 times

HOTSPOT -

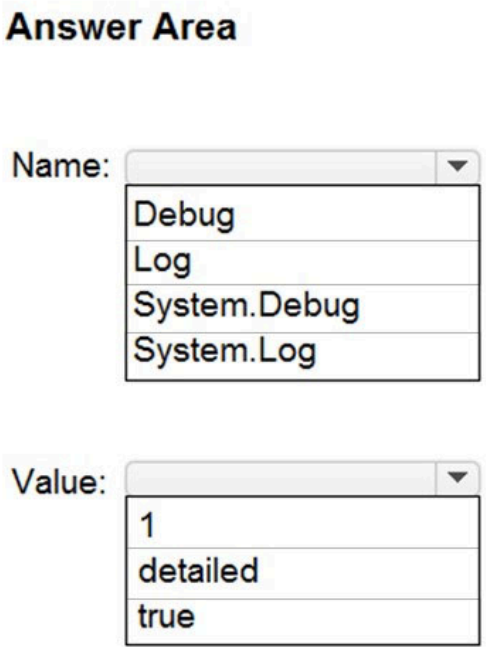
You have a project in Azure DevOps that contains a Continuous Integration/Continuous Deployment (CI/CD) pipeline.

You need to enable detailed logging by defining a pipeline variable.

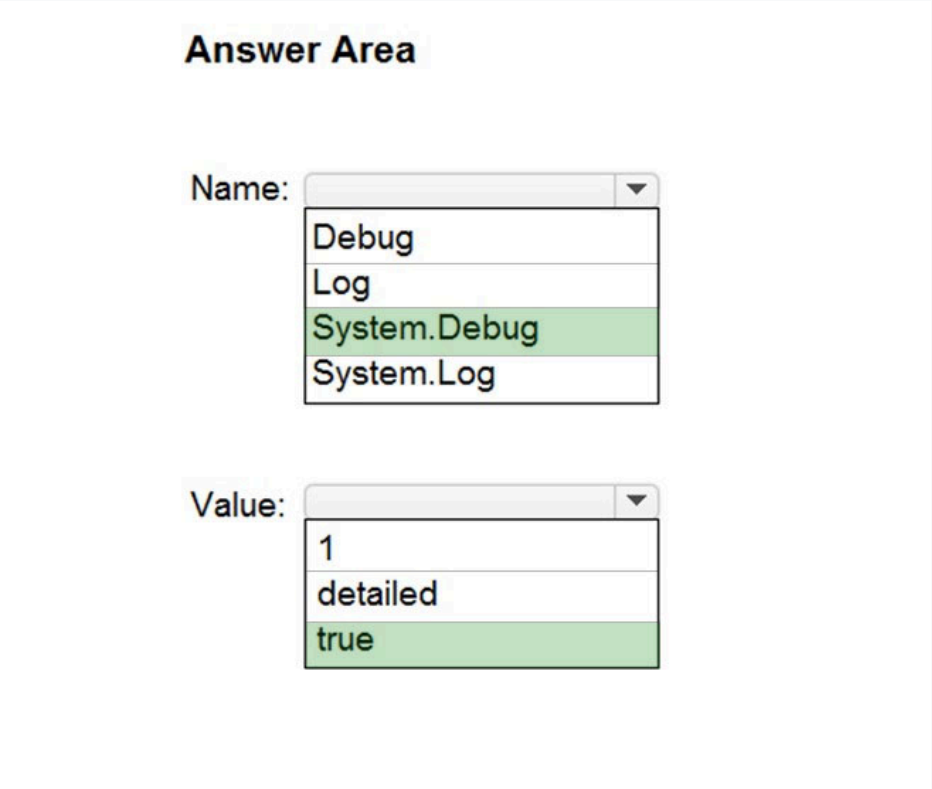
How should you configure the variable? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:



Box 1: system.debug -

To configure verbose logs for all runs, you can add a variable named system.debug and set its value to true.

Note: Verbose logging is the practice of recording to a persistent medium as much information as you possibly can about events that occur while the software runs.

Box 2: true -
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/troubleshooting/review-logs

markp Highly Voted 2 years ago
Correct. To enable verbose log you have to add the following variable:
System.Debug = true
upvoted 12 times

budha Highly Voted 1 year, 9 months ago
It was on my exam on December 7, 2022.
upvoted 7 times

resonant 1 year ago
It was on my exam too. Mine was on September 12, 2023.
upvoted 3 times

gabo 11 months, 4 weeks ago
Congrats on passing. Approx. how many questions did you get from ExamTopics?
upvoted 1 times

yusj Most Recent 3 months, 3 weeks ago
It was on my exam too. May 27, 2024.
upvoted 3 times

Firdous586 10 months, 3 weeks ago
Setting System.Debug to true configures verbose logs for all runs. You can also configure verbose logs for a single run with the Enable system diagnostics checkbox.

You can also set System.Debug to true as a variable in a pipeline or template.
upvoted 1 times

Kent_020 1 year, 2 months ago
Not sure if the setting key-value is sensitive, but from the lab, it should be 'system.debug' instead of 'System.Debug'
upvoted 1 times

gabo 11 months, 4 weeks ago
Azure Pipelines predefined variables are not case sensitive
upvoted 1 times

zellck 1 year, 3 months ago
1. System.Debug
2. true

https://learn.microsoft.com/en-us/azure/devops/pipelines/build/variables?view=azure-devops&tabs=yaml#systemdebug
For more detailed logs to debug pipeline problems, define System.Debug and set it to true.
upvoted 4 times

zellck 1 year, 3 months ago
Gotten this in Jun 2023 exam.
upvoted 7 times

JohanRojas7 1 year, 7 months ago
It was on my exam on Febrero 16, 2023.
upvoted 6 times

Ak1009 1 year, 6 months ago
Were there any labs?
upvoted 2 times

meoukg 1 year, 10 months ago
saw it yesterday in my exam
upvoted 5 times

Tidi 1 year, 8 months ago

did you get Labs?
upvoted 1 times

i_m_sushant 9 months ago
Now, in exam pattern Lab is not included. Only scenario based questions will be available
upvoted 2 times

Jaymile_1409 1 year, 9 months ago
did you get any labs ?
upvoted 3 times

syu31svc 2 years ago
Given answer is correct and link provided supports it
upvoted 1 times

hebertpena88 2 years ago
Correct!, System.Debug = true
upvoted 1 times

rinjohn 2 years ago
Correct answer.
https://docs.microsoft.com/en-us/azure/devops/pipelines/troubleshooting/review-logs?view=azure-devops#configure-verbose-logs
upvoted 1 times

Question #30 *Topic 2*

You build an iOS app.
You receive crash reports from Crashlytics.
You need to capture the following data:
➪ Crash-free users
➪ Custom events
➪ Breadcrumbs
What should you do?

A. Configure the xcworkspace file in the project

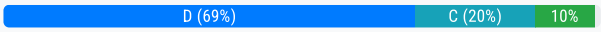
B. Add the GoogleAnalytics pod to the app.

C. Configure the Crashlytics pod in the app.

D. Import the Firebase module to UIApplicationDelegate.

Suggested Answer: *D*
Step 1: Add the Firebase Crashlytics SDK to your app.
Configure the Firebase module:
Import the Firebase module in your App struct or UIApplicationDelegate
Reference:
https://firebase.google.com/docs/crashlytics/get-started?platform=ios

Community vote distribution



pdk88 Highly Voted 2 years ago
Selected Answer: D
If you're not seeing crash-free users, breadcrumb logs, and/or velocity alerts, we recommend checking your app's configuration for Google Analytics. [...] In addition to the Firebase Crashlytics SDK, make sure that you've added the Firebase SDK for Google Analytics to your app (iOS+ | Android).
(https://firebase.google.com/docs/crashlytics/troubleshooting?platform=ios#missing-analytics-related-features)

To configure the Firebase Crashlytics SDK:

[...]Next, configure the Firebase module [...] Import the Firebase module in your App struct or UIApplicationDelegate
(https://firebase.google.com/docs/crashlytics/get-started?platform=ios#add-sdk)

Given answer D is correct.
upvoted 15 times

1sadad Highly Voted 5 months ago
Why is this question on AZ400?
upvoted 9 times

sondrex Most Recent 2 months, 3 weeks ago
To capture the required data (crash-free users, custom events, breadcrumbs) in your iOS app using Crashlytics, you need to configure the Crashlytics pod in your app.
upvoted 1 times

Pavlo 4 months, 3 weeks ago
C. Configure the Crashlytics pod in the app.

Crashlytics is a crash reporting tool provided by Firebase, which captures crash reports and additional data such as crash-free users, custom events, and breadcrumbs. By configuring the Crashlytics pod in your iOS app, you can integrate Crashlytics into your project, allowing it to capture crash reports and the specified data points. This integration typically involves adding the Crashlytics pod to your project's Podfile, installing the pod dependencies, and configuring Crashlytics initialization in your AppDelegate file
upvoted 2 times

ozbonny 6 months, 4 weeks ago

Selected Answer: D

maybe D

upvoted 1 times

ghabool 12 months ago

I choose B

This is because Google Analytics is a tool that helps you measure user behavior and satisfaction in your app, and it integrates with Firebase Crashlytics to provide features like crash-free users, custom events, and breadcrumbs1. You need to install CocoaPods dependency Manager

upvoted 1 times

Sukon_Desknot 1 year, 1 month ago

Selected Answer: C

the ans is C

By configuring the Crashlytics pod and integrating it with Firebase in your iOS app, you'll be able to capture crash-free users, custom events, and breadcrumbs effectively.

Option B (Add the GoogleAnalytics pod) and Option D (Import the Firebase module to UIApplicationDelegate) are not directly related to capturing crash data and custom events using Crashlytics, so they are not the correct choices for achieving the stated requirements

upvoted 3 times

ieboaix 1 year, 1 month ago

D. https://firebase.google.com/docs/crashlytics/get-started?platform=ios

Before you begin

If you haven't already, add Firebase to your Apple project. If you don't have an Apple app, you can download a sample app.

Recommended: To get features like crash-free users, breadcrumb logs, and velocity alerts, you need to enable Google Analytics in your Firebase project.

All Apple platforms supported by Crashlytics (except watchOS) can take advantage of these features from Google Analytics. Note that you need SDK v8.9.0+ for macOS and tvOS apps.

If your existing Firebase project doesn't have Google Analytics enabled, you can enable Google Analytics from the Integrations tab of your settings > Project settings in the Firebase console.

If you're creating a new Firebase project, enable Google Analytics during the project creation workflow.

upvoted 1 times

yana_b 1 year, 1 month ago

Selected Answer: D

Following the link provided by pdk88 I would rather go for answer D.

upvoted 1 times

zellck 1 year, 3 months ago

Selected Answer: D

D is the answer.

https://firebase.google.com/docs/crashlytics/get-started?platform=ios

upvoted 4 times

thowell 1 year, 5 months ago

Selected Answer: C

The correct answer is C. Configure the Crashlytics pod in the app.

From ChatGPT:

To capture the required data (Crash-free users, Custom events, Breadcrumbs), you need to integrate Crashlytics into your iOS app. You can do this by configuring the Crashlytics pod in the app. The Crashlytics SDK is part of the Firebase SDK, so you will also need to add the Firebase pod to your project.

A is incorrect because the xcworkspace file is a workspace configuration file and not related to Crashlytics integration.

B is incorrect because Google Analytics is a different SDK used for tracking user behavior and analytics, and not related to Crashlytics integration.

D is also incorrect because while importing the Firebase module is required for integrating Firebase in your app, it alone is not sufficient to enable Crashlytics. You still need to configure the Crashlytics pod in the app.

upvoted 3 times

jimmyyml 1 year, 6 months ago

Selected Answer: C

From chatgpt,
Option C is the correct answer because Crashlytics is a crash reporting tool that also provides features such as tracking the number of crash-free users, capturing custom events, and collecting breadcrumbs. By configuring the Crashlytics pod in the app, these features can be easily implemented and used. Option B (adding the GoogleAnalytics pod) is incorrect because it does not provide the specific features mentioned in the question. Option A (configuring the xcworkspace file) is not relevant to the question as it is a file that is automatically generated by Xcode and does not relate to the specific features required. Option D (importing the Firebase module) is also incorrect as it is not directly related to Crashlytics and does not provide the specific features mentioned in the question.

upvoted 4 times

Fal991l 1 year, 5 months ago

C is confirmed by Bing too.

upvoted 1 times

Emil_Topics 1 year, 8 months ago

Selected Answer: D

https://firebase.google.com/docs/crashlytics/troubleshooting?platform=ios#apple-platform

Make sure to include v8.9.0+ of the Firebase SDK for Google Analytics so that crashes will have access to metrics collected by Google Analytics (crash-free users, latest release, velocity alerts, and breadcrumb logs).

upvoted 4 times

budha 1 year, 9 months ago

It was on my exam on December 7, 2022.

upvoted 3 times

eliisiita1 1 year, 9 months ago

did you have labs? was it at home?

upvoted 3 times

mike_x_ 1 year, 9 months ago

Selected Answer: D

There is not Kubernetes and pods here, so D is the answer.

upvoted 3 times

Def21 2 years ago

Selected Answer: D

"you need to enable Google Analytics in your Firebase project", but it is not related to pods

upvoted 3 times

giuliohome 2 years ago

Selected Answer: D

using CocoaPods (B mentions a pod) is no longer the recommended installation method. D is well supported by the official documentation link that is provided

upvoted 3 times

Question #1 *Topic 3*

You have an Azure subscription that contains multiple Azure services.
You need to send an SMS alert when scheduled maintenance is planned for the Azure services.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Enable Azure Security Center.

B. Create and configure an Azure Monitor alert rule.

C. Create an Azure Service Health alert.

D. Create and configure an action group.

Suggested Answer: *CD*
Creating planned maintenance alerts using Azure Service Health
1. Login into the Azure portal and select Service Health.
2. Select Health alerts followed by + Create service health alert from the top of the window on the right.
3. In the Edit Alert blade, give the alert a Name, Description, check the subscription is correct and choose a resource group.
4. The next step is to work through the Criteria section choosing which services, regions and types of event alerts should be monitored. For the purpose of this article all services and regions have been checked but only planned maintenance events.
5. Select or create an Action group. (An Action group is a group of actions to be taken, should an event be logged.)
6. Configure the actions to be taken. We are only configuring an email alert, so we first name the action, then chose Email/SMS/Push/Voice from the drop down list.
Note: Azure Service Health can be used to view problems with Azure services that may impact any of your cloud services. Service Health monitors three types of health event:
Service issues ɜ€" Azure services that are currently experiencing problems
Planned maintenance ɜ€" Any known future maintenance that may affect the availability of your services
Health advisories ɜ€" Changes in services, for example, deprecated features or exceeded quota usage.
Reference:
https://www.techkb.onl/azure-using-service-health-to-alert-against-planned-maintenance/

Community vote distribution

CD (100%)

syu31svc Highly Voted 2 years, 1 month ago

Selected Answer: CD

You get the alert from an action group and service health will let you know of Azure service maintenance

Answers are C and D

upvoted 11 times

renzoku Highly Voted 1 year, 2 months ago

Selected Answer: CD

C. Create an Azure Service Health alert
Provides information about services incidents, planned maintenance and health advisories.
Creating an alert, you can receive notifications via email or SMS specifically for planned maintenance events.

D. Create and configure an action group
Define actions when an alert is triggered(e.g. send SMS notifications when Azure Service Health alert rule is triggered)

Azure Monitor alert rule, primarily focus on monitoring metrics, logs and events related to perfomance and health rather scheduled maintenance events.

upvoted 6 times

ozbonny Most Recent 6 months, 4 weeks ago

Selected Answer: CD

C and D

upvoted 1 times

yana_b 1 year, 1 month ago

Selected Answer: CD

Provided answer is correct

upvoted 2 times

codename0007 1 year, 3 months ago

C and D are correct because:

We can configure alerts for the Azure service's upcoming maintenance events. It can send a notification 24 hours before the actual event takes place. While many do not see the need for this option, most customers typically take advantage of it due to how often normal operations can change or become unpredictable.

To receive planned maintenance notification, we can follow these steps:

In the portal, select Service Health.
In the Alerts section, select Health alerts.
Select + Add service health alert and fill in the fields.
Fill out the required fields.
Choose the Event type, select Planned maintenance or Select all.
We can also add action groups to the alert rule in order to send notifications or invoke actions when a planned maintenance event is received.

upvoted 2 times

Govcomm 2 years, 1 month ago

azure service health alert and azure monitor action group (to send the SMS message)

upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 3 times

Mcelona 2 years, 4 months ago

Selected Answer: CD

It's correct

upvoted 4 times

U3 2 years, 4 months ago

Correct Answer!

upvoted 3 times

U3 2 years, 4 months ago

I think B&D?

upvoted 2 times

U3 2 years, 4 months ago

My fault, please ignore

upvoted 3 times

Question #2 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure DevOps organization named Contoso and an Azure subscription. The subscription contains an Azure virtual machine scale set named VMSS1 that is configured for autoscaling.
You have a project in Azure DevOps named Project1. Project1 is used to build a web app named App1 and deploy App1 to VMSS1.
You need to ensure that an email alert is generated whenever VMSS1 scales in or out.
Solution: From Azure Monitor, configure the autoscale settings.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Instead create an action group.
Note: An action group is a collection of notification preferences defined by the owner of an Azure subscription. Azure Monitor, Service Health and Azure Advisor alerts use action groups to notify users that an alert has been triggered.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups

Community vote distribution
B (57%) A (43%)

Lucky_me Highly Voted 2 years, 2 months ago
Selected Answer: B
Action group is the correct solution
upvoted 6 times

Tyler2023 1 year, 1 month ago
I think you don't need an action group, you only need to check the box for "Email administrators", "Email co-administrator", or add email on the text field based on this
https://www.trendmicro.com/cloudoneconformity/knowledge-base/azure/VirtualMachines/enable-autoscale-notifications.html
upvoted 5 times

catfood 1 year, 1 month ago
agree. https://learn.microsoft.com/en-us/azure/azure-monitor/autoscale/autoscale-webhook-email?tabs=portal
upvoted 3 times

AugustineUba Most Recent 2 months ago
Selected Answer: A
Microsoft documentation clearly states "Use autoscale actions to send email and webhook alert notifications in Azure Monitor" form the topic in the below link
https://learn.microsoft.com/en-us/azure/azure-monitor/autoscale/autoscale-webhook-email?tabs=portal
So correct answer is A
upvoted 2 times

ay_m 3 months, 1 week ago
Selected Answer: A
Intuitively I would say an action group is needed, but apparently you can configure this directly from the autoscale settings

https://learn.microsoft.com/en-us/azure/azure-monitor/autoscale/autoscale-webhook-email?tabs=portal
upvoted 3 times

ozbonny 6 months, 4 weeks ago
Selected Answer: B

A configures the auto scale that is fine but to send alerts you need to configure the action from action groups to send email
upvoted 1 times

vsvaid 8 months, 3 weeks ago

Selected Answer: A

The email alert can be configured so yes.
https://learn.microsoft.com/en-us/azure/azure-monitor/autoscale/autoscale-webhook-email?tabs=portal
upvoted 2 times

vsvaid 9 months ago

https://learn.microsoft.com/en-us/azure/azure-monitor/autoscale/autoscale-webhook-email?tabs=portal
upvoted 1 times

gabo 11 months, 3 weeks ago

From Autoscale settings, choose option to send email and that requires to setup an action group. So the answer is partially yes and partially no, really confusing.
upvoted 3 times

yana_b 1 year, 1 month ago

Selected Answer: B

Use an action group instead
upvoted 1 times

catfood 1 year, 1 month ago

Selected Answer: A

Set up notifications using the Azure portal.
Select the Notify tab on the autoscale settings page to configure notifications.

Select the check boxes to send an email to the subscription administrator or co-administrators. You can also enter a list of email addresses to send notifications to.

https://learn.microsoft.com/en-us/azure/azure-monitor/autoscale/autoscale-webhook-email?tabs=portal
upvoted 1 times

Tyler2023 1 year, 1 month ago

My answer is A, you need to first configure the auto-scale before you can setup any notification

https://www.trendmicro.com/cloudoneconformity/knowledge-base/azure/VirtualMachines/enable-autoscale-notifications.html
upvoted 1 times

PravinDhote 1 year, 8 months ago

Selected Answer: B

ANS B - Action group is needed.
upvoted 2 times

Sam90765 1 year, 8 months ago

Selected Answer: A

I think it is Yes; https://www.trendmicro.com/cloudoneconformity/knowledge-base/azure/VirtualMachines/enable-autoscale-notifications.html
upvoted 2 times

Tyler2023 1 year, 1 month ago

yeah, I also think it is Yes, you need to first configure the auto-scale, I also saw this message on my VMSS resource
upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: B

No for sure

Action group is needed
upvoted 1 times

kennynelcon 2 years, 1 month ago

Selected Answer: B

Email alert means you need an action group
upvoted 2 times

Question #3 *Topic 3*

You configure Azure Application Insights and the shared service plan tier for a web app.
You enable Smart Detection.
You confirm that standard metrics are visible in the logs, but when you test a failure, you do not receive a Smart Detection notification.
What prevents the Smart Detection notification from being sent?

A. You must enable the Snapshot Debugger for the web app.

B. Smart Detection uses the first 24 hours to establish the normal behavior of the web app.

C. The web app is configured to use the shared service plan tier.

D. You must restart the web app before Smart Detection is enabled.

Suggested Answer: *B*
After setting up Application Insights for your project, and if your app generates a certain minimum amount of data, Smart Detection of failure anomalies takes 24 hours to learn the normal behavior of your app, before it is switched on and can send alerts.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/proactive-failure-diagnostics

Community vote distribution
B (100%)

ozbonny 6 months, 4 weeks ago
Selected Answer: B
ok then B
upvoted 3 times

yana_b 1 year, 1 month ago
Selected Answer: B
Provided answer is correct
upvoted 1 times

all_cloud 1 year, 2 months ago
B is the correct answer.
upvoted 1 times

Pavlo 1 year, 3 months ago
The correct answer is B. Smart Detection uses the first 24 hours to establish the normal behavior of the web app.
upvoted 1 times

xRiot007 1 year, 2 months ago
Is that the only reason for preventing Smart Detection ? The requirement does not specify that we look for failures after or before 24 hours.
upvoted 1 times

Matharax 1 year, 11 months ago
Selected Answer: B
Takes 24 to collect data.
upvoted 4 times

syu31svc 2 years, 1 month ago
Selected Answer: B
B is correct as supported by given explanation and link
upvoted 1 times

Govcomm 2 years, 1 month ago
It requires 24 hours to collect the data.
upvoted 1 times

Mcelona 2 years, 4 months ago
Selected Answer: B
It's Correct
upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 1 times

ppo12 2 years, 4 months ago

Looks good to me

upvoted 1 times

mclovin 2 years, 4 months ago

makes sense

upvoted 1 times

U3 2 years, 4 months ago

Correct!

upvoted 1 times

yassine125 2 years, 4 months ago

B : Après avoir configuré Application Insights pour votre projet , et si votre application génère un certain minimum de données, la détection intelligente des anomalies de défaillance prend 24 heures pour apprendre le comportement normal de votre application, avant qu'elle ne soit allumée et puisse envoyer des alertes.

upvoted 1 times

Question #4 *Topic 3*

DRAG DROP -

You are planning projects for three customers. Each customer's preferred process for work items is shown in the following table.

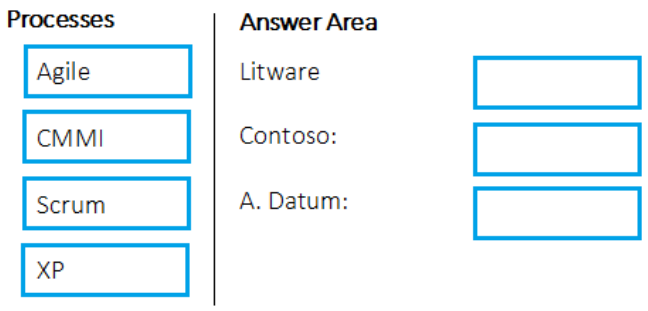
Customer name	Preferred process
Litware, Inc.	Track product backlog items (PBIs) and bugs on the Kanban board. Break the PBIs down into tasks on the task board.
Contoso, Ltd.	Track user stories and bugs on the Kanban board. Track the bugs and tasks on the task board.
A. Datum Corporation	Track requirements, change requests, risks, and reviews.

The customers all plan to use Azure DevOps for work item management.

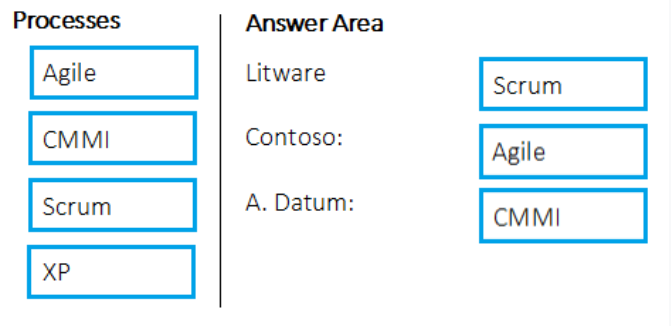
Which work item process should you use for each customer? To answer, drag the appropriate work item processes to the correct customers. Each work item process may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested Answer:



Box 1: Scrum -

Choose Scrum when your team practices Scrum. This process works great if you want to track product backlog items (PBIs) and bugs on the Kanban board, or break PBIs and bugs down into tasks on the taskboard.

Box 2: Agile -

Choose Agile when your team uses Agile planning methods, including Scrum, and tracks development and test activities separately. This process works great if you want to track user stories and (optionally) bugs on the Kanban board, or track bugs and tasks on the taskboard.

Box 3: CMMI -

Choose CMMI when your team follows more formal project methods that require a framework for process improvement and an auditable record of decisions. With this process, you can track requirements, change requests, risks, and reviews.

Incorrect Answers:

XP:

The work tracking objects contained within the default DevOps processes and DevOps process templates are Basic, Agile, CMMI, and Scrum

XP (Extreme Programming) and DevOps are different things. They don't contradict with each other, they can be used together, but they have different base concepts inside them.

Reference:

https://docs.microsoft.com/en-us/azure/devops/boards/work-items/guidance/choose-process?view=azure-devops

AS007 Highly Voted 4 years, 4 months ago

Verified - its correct

upvoted 44 times

Govcomm Highly Voted 2 years, 1 month ago
product backlog --> scrum
user stories --> Agile
track changes --> CMMI
upvoted 16 times

ozbonny Most Recent 6 months, 4 weeks ago
correct
upvoted 1 times

vsvaid 9 months ago
Provided answer is correct
upvoted 1 times

yana_b 1 year, 1 month ago
Provided answer is correct
upvoted 1 times

meoukg 1 year, 10 months ago
saw it yesterday in my exam
upvoted 5 times

syu31svc 2 years, 1 month ago
Answer is correct and provided link supports it
upvoted 1 times

Leandrocei 2 years, 2 months ago
Correct. Came today 22 july 9
upvoted 1 times

Mcelona 2 years, 4 months ago
It's correct
upvoted 2 times

UnknowMan 2 years, 4 months ago
Correct
upvoted 1 times

Cheehp 2 years, 5 months ago
Selected during exam. Scrum, Agile, CMMI
upvoted 1 times

rdemontis 2 years, 5 months ago
correct answer
upvoted 1 times

[Removed] 2 years, 9 months ago
Some how it looks like Scrum can fit for contoso ?
upvoted 1 times

ScreamingHand 2 years, 10 months ago
Came in today 5th Nov 2021
upvoted 2 times

wasthi 2 years, 10 months ago
It's better if you can mentioned you given answered also with your comment, because you passed mean your answer is correct, it will kind help for all of us.
upvoted 2 times

Anoop_Pandathil 3 years, 7 months ago
Verified
upvoted 3 times

RKS 3 years, 7 months ago
Verified - Correct!
upvoted 2 times

Jkmr622 3 years, 8 months ago

Scrum

agile

CMMI

Es correctamundo dude

upvoted 5 times

Question #5 *Topic 3*

You configure an Azure Application Insights availability test.
You need to notify the customer services department at your company by email when availability is degraded.
You create an Azure logic app that will handle the email and follow up actions.
Which type of trigger should you use to invoke the logic app?

A. an HTTPWebhook trigger

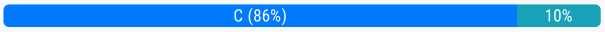
B. an HTTP trigger

C. a Request trigger

D. an ApiConnection trigger

Suggested Answer: *A*
You can use webhooks to route an Azure alert notification to other systems for post-processing or custom actions. You can use a webhook on an alert to route it to services that send SMS messages, to log bugs, to notify a team via chat or messaging services, or for various other actions.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-webhooks

Community vote distribution



rdemontis Highly Voted 2 years, 6 months ago

Selected Answer: C

Correct answer is C. Probably the following article has generated a misunderstanding:

https://docs.microsoft.com/en-us/azure/app-service/tutorial-send-email?tabs=dotnet

It uses the Action "When an HTTP request is received" and defines it as HTTP Request trigger. But this is a Request Trigger and not an HTTP Trigger.
Please look at the document below where it is explained the difference very well.

https://docs.microsoft.com/en-us/azure/connectors/connectors-native-reqres

You have to consider that http trigger is used only for outbound requests from the logic app. You can't use it for Inbound http requests. For those you have to use Request Trigger.
upvoted 53 times

pdk88 2 years ago
It's exactly as you say:

inbound HTTP requests TO the logic app, trigger it to do things
outbound HTTP triggers FROM the logic app can trigger other endpoints or services

https://docs.microsoft.com/en-us/azure/connectors/connectors-native-reqres?tabs=consumption
https://docs.microsoft.com/en-us/azure/connectors/connectors-native-http

C is the right answer
upvoted 4 times

giuliohome 2 years ago
Yeah, you're right but Microsoft terminology is very misleading and non-standard. But yes, answer is C, thank you for your explanation, notice that the link for the outbound "http trigger" is here: https://docs.microsoft.com/en-us/azure/connectors/connectors-native-http#http-trigger
upvoted 2 times

RealRaymond 1 year, 3 months ago
Yes, C is correct. More info here: https://learn.microsoft.com/en-us/azure/logic-apps/logic-apps-examples-and-scenarios

upvoted 2 times

Hooters Highly Voted 3 years, 10 months ago

Should be B.- HTTP trigger

https://docs.microsoft.com/en-us/azure/app-service/tutorial-send-email?tabs=dotnet

upvoted 53 times

az_cli 3 years, 6 months ago

agree with you :

https://dailydotnettips.com/sending-your-azure-application-insights-alerts-to-team-sites-using-azure-logic-app/

upvoted 6 times

marmila Most Recent 1 month, 1 week ago

Selected Answer: C

answer is C: https://learn.microsoft.com/en-us/azure/logic-apps/business-continuity-disaster-recovery-guidance?wt.mc_id=knwlserapi_inproduct_azportal#trigger-type-guidance

upvoted 1 times

marmila 1 month, 1 week ago

Answer is C: https://learn.microsoft.com/en-us/azure/logic-apps/business-continuity-disaster-recovery-guidance?wt.mc_id=knwlserapi_inproduct_azportal#trigger-type-guidance

upvoted 1 times

4bd3116 4 months, 3 weeks ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/app-service/tutorial-send-email?tabs=python

upvoted 1 times

ozbonny 6 months, 4 weeks ago

Selected Answer: C

Correct answer C

upvoted 1 times

vsvaid 8 months, 3 weeks ago

Selected Answer: C

It is Request Trigger

upvoted 1 times

ObiWan500 10 months ago

Selected Answer: B

The Logic App will be triggered by an Action Group as an HTTP request.

upvoted 2 times

yana_b 11 months ago

Selected Answer: C

https://learn.microsoft.com/en-us/azure/app-service/tutorial-send-email?tabs=dotnet

upvoted 1 times

hristozkov69 11 months, 1 week ago

The question is "which TYPE of trigger". The HTTP request trigger in the logic app configuration is a Request Type trigger, so C is the correct answer.

upvoted 1 times

yuu_oppai 11 months, 2 weeks ago

Selected Answer: B

Should be B.- HTTP trigger

https://docs.microsoft.com/en-us/azure/app-service/tutorial-send-email?tabs=dotnet

upvoted 2 times

Oreao 11 months, 2 weeks ago

A. an HTTPWebhook trigger

You can configure Azure Application Insights to send an HTTP webhook when availability is degraded, and this trigger will invoke the logic app when the webhook is received. Inside the logic app, you can set up actions to send email notifications and perform any follow-up actions required.

Option B, an HTTP trigger, is used when you want to initiate a logic app manually or through an HTTP request but doesn't directly connect to Azure Application Insights for event-based triggers.
upvoted 2 times

peekingpicker 11 months, 4 weeks ago
"Under the Start with a common trigger section, select the trigger named When an HTTP request is received ."

HTTP Request is B, isn't it ?
or just Request as in C ? but just "Request" could also mean API Request, isn't it ?
upvoted 1 times

ghabool 12 months ago
I choose A

This is because an HTTPWebhook trigger can subscribe to an external service and wait for a callback from that service before continuing the logic app's workflow. In this case, the external service is the Application Insights availability test, which can send an alert to a webhook URL when availability is degraded. The logic app can use the HTTPWebhook trigger to provide the webhook URL and receive the alert payload from the availability test. Then, the logic app can use other actions to handle the email and follow up actions. An HTTP trigger, on the other hand, is used to start a logic app when it receives an HTTP request from any source. A Request trigger is used to start a logic app when it receives a request from another logic app or a Power Automate flow. An ApiConnection trigger is used to start a logic app when it connects to an API, such as Office 365 or Dropbox. These triggers are not suitable for invoking the logic app based on the availability test alert.
upvoted 1 times

d78b459 1 year, 1 month ago
Selected Answer: C
Correct answer is C.

HTTPWebhook trigger
This trigger makes your logic app callable by creating an endpoint that can register a subscription by calling the specified endpoint URL. When you create this trigger in your workflow, an outgoing request makes the call to register the subscription.

HTTP trigger
This trigger sends a request to the specified HTTP or HTTPS endpoint based on the specified recurrence schedule. The trigger then checks the response to determine whether the workflow runs.

Request trigger
This trigger makes your logic app callable by creating an endpoint that can accept incoming requests.

https://learn.microsoft.com/en-us/azure/logic-apps/logic-apps-workflow-actions-triggers
upvoted 4 times

renzoku 1 year, 2 months ago
Selected Answer: C
C. a Request trigger

1. Azure Application Insights availability test -> HTTP request(Request trigger, when availability is degraded)
2. Logic app, send an email notification -> customer
In Logic app you define the endpoint URL that will receive the HTTP request (from the availability test)
upvoted 2 times

Rouix 1 year, 2 months ago
Looks like this should be C.
According to the documentation: The Request trigger creates a manually callable endpoint that can handle only inbound requests over HTTPS. When the calling service sends a request to this endpoint, the Request trigger fires and runs the logic app workflow.
https://learn.microsoft.com/en-us/azure/connectors/connectors-native-reqres?tabs=consumption
upvoted 1 times

Question #6 *Topic 3*

You have an Azure DevOps organization named Contoso and an Azure subscription.
You use Azure DevOps to build a containerized app named App1 and deploy App1 to an Azure container instance named ACI1.
You need to restart ACI1 when App1 stops responding.
What should you do?

A. Add a liveness probe to the YAML configuration of App1.

B. Add a readiness probe to the YAML configuration of App1.

C. Use Connection Monitor in Azure Network Watcher.

D. Use IP flow verify in Azure Network Watcher.

Suggested Answer: *B*
For containerized applications that serve traffic, you might want to verify that your container is ready to handle incoming requests. Azure Container Instances supports readiness probes to include configurations so that your container can't be accessed under certain conditions. The readiness probe behaves like a
Kubernetes readiness probe. For example, a container app might need to load a large data set during startup, and you don't want it to receive requests during this time.
YAML is used to setup a liveness probe.
Reference:
https://docs.microsoft.com/en-us/azure/container-instances/container-instances-readiness-probe

Community vote distribution

A (100%)

SkyDream Highly Voted 3 years, 10 months ago
Should be A Liveness Probe
https://docs.microsoft.com/en-us/azure/container-instances/container-instances-liveness-probe
upvoted 80 times

Appsuri Highly Voted 3 years, 10 months ago
Answer is A
upvoted 19 times

ablioma Most Recent 2 months, 2 weeks ago
Selected Answer: A
A is correct
upvoted 1 times

ozbonny 6 months, 4 weeks ago
Selected Answer: A
Correct A since it need to restart if it fails
upvoted 2 times

ozbonny 6 months, 4 weeks ago
Selected Answer: A
for me is A
upvoted 1 times

vsvaid 9 months ago
Selected Answer: A
Liveness Probe
upvoted 1 times

UtsavShah01 1 year, 1 month ago
Selected Answer: A
Liveness probe to restart the container
upvoted 1 times

flafernan 1 year, 1 month ago

57. When using Helth check in Kubernets, there are two types of resources:
- Readiness probe: this feature is used during the creation of a new pod, where it informs if the pods in question can already receive “requests”.
- Liveness probe: here is a process to know if the pods are live or inactive. It is this feature that configures the automatic restart when the power stops responding.
upvoted 6 times

Lence123 1 year, 2 months ago
A liveness probe is a diagnostic tool used to check the health of a container and determine if it is running properly. By adding a liveness probe to the YAML configuration of App1, you can periodically check if the application is responsive. If the liveness probe fails, indicating that the application is not responding, Azure DevOps can automatically restart ACI1.
upvoted 1 times

ShomaV 1 year, 3 months ago
If your main goal is to restart the container when the application within it becomes unresponsive or enters an invalid state, then you should include a liveness probe in the YAML configuration of App1.
upvoted 1 times

cluqueg 1 year, 4 months ago
Selected Answer: A
Agree on A
upvoted 1 times

RonZhong 1 year, 4 months ago
(A) Liveness Probe - To restart the instance

Both liveness & readiness probes are used to control the health of an application. Failing liveness probe will restart the container, whereas failing readiness probe will stop our application from serving traffic.
upvoted 1 times

mohiniu 1 year, 6 months ago
Answer should be liveness container. As in case of readiness probe failure , container is never restarted.But only traffic is not send to the container. Only in case of liveness probe , container is restarted.
upvoted 1 times

mohiniu 1 year, 6 months ago
Typo: Liveness probe**
upvoted 1 times

fkaracan 1 year, 7 months ago
Selected Answer: A
A. Add a liveness probe to the YAML configuration of App1.

A liveness probe is used to detect when an application is no longer responding and take action to restart the application, such as restarting the container. By adding a liveness probe to the YAML configuration of App1, you can configure the probe to check if the application is responding and if not, trigger a restart of the container instance ACI1.
upvoted 1 times

AshutoshSingh 1 year, 8 months ago
Simply put
ReadinessProbe will check the app until its active once it gets confirmation it will loop out
Liveness Probe will come into play after the ReadinessProbe & it will keep on checking the application until it stops.
upvoted 3 times

Matharax 1 year, 11 months ago
Selected Answer: A
When it stops responding, not check if is ready to take requests. Should be 'Liveliness probe'.
upvoted 2 times

VladanO 2 years ago
https://faun.pub/the-difference-between-liveness-readiness-and-startup-probes-781bd3141079
Liveness Probes: Used to check if the container is available and alive.
Readiness Probes: Used to check if the application is ready to use and serve the traffic.
>>You need to restart ACI1 when App1 stops responding.
Correct answer is B.

upvoted 2 times

VladanO 2 years ago

Delete this comment, the question is about the container ACI1, correct answer is A

upvoted 1 times

Question #7 *Topic 3*

You have a multi-tier application that has an Azure Web Apps front end and an Azure SQL Database back end.
You need to recommend a solution to capture and store telemetry data. The solution must meet the following requirements:
➪ Support using ad-hoc queries to identify baselines.
➪ Trigger alerts when metrics in the baseline are exceeded.
➪ Store application and database metrics in a central location.
What should you include in the recommendation?

A. Azure Event Hubs

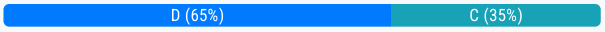
B. Azure SQL Database Intelligent Insights

C. Azure Application Insights

D. Azure Log Analytics

Suggested Answer: *D*
Azure Platform as a Service (PaaS) resources, like Azure SQL and Web Sites (Web Apps), can emit performance metrics data natively to Log Analytics.
The Premium plan will retain up to 12 months of data, giving you an excellent baseline ability.
There are two options available in the Azure portal for analyzing data stored in Log analytics and for creating queries for ad hoc analysis.
Incorrect Answers:
B: Intelligent Insights analyzes database performance by comparing the database workload from the last hour with the past seven-day baseline workload.
However, we need handle application metrics as well.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/collect-azurepass-posh

Community vote distribution



gulopez Highly Voted 3 years, 9 months ago
I think answer should be Log Analytics
What kind of telemetry data is being handled by Log Analytics ? -> Data related to infrastructure and network level i.e., few of them are syslogs, IIS logs, custom logs, windows events, windows and linux performance counters, etc. For more information, please refer https://docs.microsoft.com/en-us/azure/azure-monitor/azure-monitor-log-hub

What kind of telemetry data is being handled by App Insights ? -> Data related to code-level application performance level i.e., few of them are ping URL tests, page view counts, page view load data, HTTP requests, dependency calls, exceptions and stack traces, custom events and metrics that you code, trace logs, AJAX calls, user and session counts, run-time exceptions, failure anomalies, abnormal rise in exceptions, etc. For more information, please refer https://docs.microsoft.com/en-us/azure/azure-monitor/azure-monitor-app-hub and https://docs.microsoft.com/en-us/azure/azure-monitor/app/troubleshoot-faq#what-telemetry-is-collected-by-application-insights
upvoted 24 times

armvch 1 year, 6 months ago
We need to store application and database metrics. According to provided links app logs should be handled by App Insights. Why did you choose LA then
upvoted 3 times

msuleman92 Highly Voted 4 years, 3 months ago
Its C, Cause in Log Analytics you can run the Queries + You can set triggers for alerts. and centralized Database Management.
upvoted 9 times

ozbonny Most Recent 6 months, 4 weeks ago
Selected Answer: D
I think D since we need both metrics UI and SQL
upvoted 1 times

vsvaid 8 months, 3 weeks ago
Selected Answer: D

Log analytics for me. Someone mentioned in the comments that we cannot create alert rules in log. That is incorrect, we can create alerts on custom log queries just like insight alert rules

upvoted 2 times

gcgonzales 8 months, 3 weeks ago

Selected Answer: D

Both Log Analytics and Application Insights meets almost all requirements EXCEPT database Telemetry. This is only achieved via Log Analytics, while Application Insights track dependencies with SQL services, but almost no more.

Answer: D. Log Analytics

upvoted 4 times

vsvaid 9 months ago

Selected Answer: D

Log Analytics--
Application Insights does not store data. Application Insights is a layer on top of Log Analytics aimed at application-level telemetry and uses the log data stored in Log Analytics to provide an additional bunch of features that make App Insights an Application Performance Management tool

upvoted 1 times

yuu_oppai 11 months, 2 weeks ago

Selected Answer: C

It is C.

upvoted 2 times

Tyler2023 1 year ago

Does Application Insights store database metrics? I think no,
but one of the requirements is "Store application and database metrics in a central location."
I'm not familiar with Azure SQL Database Intelligent Insights but I assume it only cares about the database logs and metrics
Azure Event Hubs, you can't use ad-hoc queries
So the answer is Azure Log Analytics

upvoted 1 times

Sukon_Desknot 1 year, 1 month ago

Selected Answer: C

Log Analytics will not "Trigger alerts when metrics in the baseline are exceeded."

upvoted 2 times

flafernan 1 year, 1 month ago

C and D: While both Azure Application Insights and Log Analytics can meet the question's requirements, Microsoft likely chose to consider Log Analytics as the correct answer because it is more widely used for collecting and analyzing telemetry data in cloud environments. Log Analytics is a powerful tool that provides advanced analytics and insights to help monitor and troubleshoot cloud applications and infrastructure. Additionally, Log Analytics is highly integrated into the Azure ecosystem, making it a natural choice for this type of scenario. However, it is important to note that Azure Application Insights is also a valid and effective option for capturing and analyzing telemetry data in web applications. Both solutions can be successfully used to meet the requirements mentioned in the question.

upvoted 2 times

renzoku 1 year, 2 months ago

Selected Answer: D

Apparently the answer is:
D. Azure Log Analytics
>Collecting, storing, and analyzing log data from various sources (Multi-tier application)
>Powerful query language for querying log data (Support using ad-hoc queries to identify baselines)
>Alerts based on log data (Trigger alerts when metrics in the baseline are exceeded)
>Centralize and correlate logs for monitoring, troubleshooting across your environment (Store application and database metrics in a central location)

Azure Application Insights, focused on application performance monitoring, well-suited for monitoring web applications, APIs(doesn't fit to multi-tier applications as well as Log Analytics), and itself is not a centralized location for storing data.

upvoted 4 times

DHAdmin 1 year, 6 months ago

Selected Answer: C

from chatGPT: However, Azure Log Analytics does not provide some of the advanced application monitoring capabilities that are available in Azure Application Insights, such as automatic collection of telemetry data from web apps and services, and built-in support for identifying and diagnosing performance and availability issues.
upvoted 4 times

Fal991l 1 year, 4 months ago
Option D, **Azure Log Analytics**, is not the best solution for capturing and storing telemetry data in this scenario because it is primarily used for collecting and analyzing data from different sources . It does not support ad-hoc queries to identify baselines or trigger alerts when metrics in the baseline are exceeded . It also does not store application and database metrics in a central location .

Therefore, Azure Log Analytics does not meet all of the requirements for capturing and storing telemetry data.

References:
: Microsoft. (n.d.). What is Log Analytics? https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-overview
upvoted 2 times

jimmyyml 1 year, 6 months ago
Selected Answer: C
C.
From chatgpt,
Based on the requirements, the best recommendation would be to use Azure Application Insights. Application Insights supports ad-hoc queries and alerting when metrics exceed baselines. It also stores application and database metrics in a central location, making it easy to monitor and analyze the data. While Azure Log Analytics could also be used to store and analyze telemetry data, it does not have built-in support for ad-hoc queries or alerting based on metrics exceeding baselines. Azure Event Hubs is primarily used for event streaming and real-time data ingestion, and while Azure SQL Database Intelligent Insights provides database performance monitoring and recommendations, it does not support monitoring of the application tier or alerting based on metrics exceeding baselines.
upvoted 1 times

mohamed1999 2 years ago
Selected Answer: D
they have a condition "Store application and database metrics in a central location."

Application Insights is not a centralised location. There for Log Analytics is correct.
upvoted 4 times

coffecold 1 year, 10 months ago
Application Insights can store data in Log Analytics workspaces
upvoted 1 times

armvch 1 year, 6 months ago
Yes, but why should we choose AI then? If we use Log Analytics for storing
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: D
This is D for sure
upvoted 2 times

kennynelcon 2 years, 1 month ago
Selected Answer: D
Log Analytics is the accurate answer, as it stores data related to network
upvoted 2 times

Govcomm 2 years, 1 month ago
azure log analytics
upvoted 2 times

Question #8 *Topic 3*

You have an Azure DevOps organization named Contoso and an Azure subscription. The subscription contains an Azure virtual machine scale set named VMSS1 that is configured for autoscaling.
You use Azure DevOps to build a web app named App1 and deploy App1 to VMSS1. App1 is used heavily and has usage patterns that vary on a weekly basis.
You need to recommend a solution to detect an abnormal rise in the rate of failed requests to App1. The solution must minimize administrative effort.
What should you include in the recommendation?

A. the Smart Detection feature in Azure Application Insights

B. the Failures feature in Azure Application Insights

C. an Azure Service Health alert

D. an Azure Monitor alert that uses an Azure Log Analytics query

Suggested Answer: *A*
After setting up Application Insights for your project, and if your app generates a certain minimum amount of data, Smart Detection of failure anomalies takes 24 hours to learn the normal behavior of your app, before it is switched on and can send alerts.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/proactive-failure-diagnostics

Community vote distribution
A (100%)

kumardeb Highly Voted 3 years, 10 months ago
A. the Smart Detection feature in Azure Application Insights
upvoted 18 times

Marang73 Highly Voted 3 years, 10 months ago
Answer A. Smart dection has a standard rule named "Abnormal rise in exception volume" which can alert by e-mail. With feature Failures (answer B) you have to search by your own for exceptions.
upvoted 6 times

syu31svc Most Recent 2 years, 1 month ago
Selected Answer: A
"minimize administrative effort"

I would take A as the answer
upvoted 1 times

Govcomm 2 years, 1 month ago
abnormal application behaviors --> Application Insights Smart Detection.
upvoted 1 times

UnknowMan 2 years, 4 months ago
Correct
upvoted 1 times

rdemontis 2 years, 6 months ago
Selected Answer: A
correct A
https://docs.microsoft.com/en-us/azure/azure-monitor/app/proactive-diagnostics
upvoted 2 times

shermin1 2 years, 6 months ago
Came in exam march 13....
upvoted 2 times

lugospod 2 years, 7 months ago
Got this January 2022.

upvoted 1 times

Pankaj78 2 years, 9 months ago

Selected Answer: A

A. the Smart Detection feature in Azure Application Insights

upvoted 5 times

RajatSahani 2 years, 9 months ago

smart detection

upvoted 1 times

AZ5cert 2 years, 12 months ago

Correct

upvoted 2 times

megaejay 3 years, 2 months ago

it's a web app hosted on a vmss.

A is correct because , it's possible to install insight agent on vm/vmss ...

https://blog.hametbenoit.info/2019/11/05/azure-you-can-now-deploy-azure-monitor-application-insights-agent-on-azure-virtual-machine-and-azure-virtual-machine-scale-sets/#.YNkMl-gzZPY

upvoted 3 times

jay158 2 years, 5 months ago

Link not working now

upvoted 1 times

theboywonder 3 years, 4 months ago

A is correctamundo dude

upvoted 1 times

27close 3 years, 10 months ago

Application Insights automatically alerts you in near real time if your web app experiences an abnormal rise in the rate of failed requests. It detects an unusual rise in the rate of HTTP requests or dependency calls that are reported as failed.

upvoted 3 times

Question #9 *Topic 3*

SIMULATION -
You need to ensure that Microsoft Visual Studio 2017 can remotely attach to an Azure Function named fa-11566895.
To complete this task, sign in to the Microsoft Azure portal.

Suggested Answer: *See explanation below.*
Enable Remote Debugging -
Before we start a debugging session to our Azure Function app we need to enable the functionality.
1. Navigate in the Azure portal to your function app fa-11566895
2. Go to the ı€Application settingsı€
3. Under ı€Debuggingı€ set Remote Debugging to On and set Remote Visual Studio version to 2017.
Reference:
https://www.locktar.nl/uncategorized/azure-remote-debugging-manually-in-visual-studio-2017/

Mithi Highly Voted 3 years, 10 months ago
1. Navigate in the Azure portal to your function app fa-11566895 and click on Configuration in left panel
2. Go to the "General settings"
3. Under "Debugging" set Remote Debugging to On and set Remote Visual Studio version to 2017.
upvoted 41 times

mrsmjparker 3 years, 9 months ago
12/18 I verified Mithi's answer and it is correct
upvoted 2 times

rdemontis 2 years, 5 months ago
correct
upvoted 1 times

yana_b 1 year, 1 month ago
These steps are still valid, just there are more options for VS versions, including 2022.
upvoted 1 times

Pinky777 Most Recent 11 months ago
I guess it'll be enabled only if function app is deployed
https://jamiemaguire.net/index.php/2023/07/08/how-to-remote-debug-a-deployed-azure-function/
upvoted 1 times

Pinky777 11 months ago
This does not work for Azure function app. These steps work for regular azure web application
upvoted 1 times

pc1707 1 year, 1 month ago
1. Navigate in the Azure portal to your function app fa-11566895 and click on Configuration in left panel
2. Go to the "General settings"
3. Under "Debugging" set Remote Debugging to On and set Remote Visual Studio version to 2017.
https://youtu.be/kuPreUIHx4A
upvoted 1 times

yana_b 1 year, 1 month ago
1. go to your function app in AZ portal
2. under 'Settings' select 'Configuration'
3. Go to General settings tab
4. Under Debugging set remote debugging to "on"
5. If required, select VS version
upvoted 2 times

waqy 1 year, 2 months ago
Question. how do we attempt to do these simulations questions in real exam ? do we have to remember the steps and we have to write these steps in exam ?
upvoted 3 times

Atos 2 years ago

Select Function

Go to Settings/Configuration

General Settings/Remote Debugging - On

upvoted 3 times

SerdarG 2 years, 1 month ago

https://docs.microsoft.com/en-us/answers/questions/296869/how-to-remote-debugg-an-azure-function-that-we-tri.html

upvoted 1 times

Ajitdh 2 years, 1 month ago

1. Navigate in the Azure portal to your function app fa-11566895
2. Go to the "configuration" then "general settings "
3. Under "Debugging" set Remote Debugging to On and set Remote Visual Studio version to 2017.

upvoted 2 times

Govcomm 2 years, 1 month ago

Azure Functions --> Settings --> Configuration --> Remote debugging

upvoted 3 times

Dsyadav 3 years, 5 months ago

settings>configurations>general settings>remote debugging>click on radio button

upvoted 2 times

Kolego 2 years, 11 months ago

no enough, you need to also choose proper VS version.

upvoted 4 times

Question #10 *Topic 3*

You have an Azure subscription that contains resources in several resource groups.
You need to design a monitoring strategy that will provide a consolidated view. The solution must support the following requirements:
➪ Support role-based access control (RBAC) by using Azure Active Directory (Azure AD) identifies.
➪ Include visuals from Azure Monitor that are generated by using the Kusto query language.
➪ Support documentation written in markdown.
➪ Use the latest data available for each visual.
What should you use to create the consolidated view?

A. Azure Monitor

B. Microsoft Power BI

C. Azure Data Explorer

D. Azure dashboards

Suggested Answer: *C*
There are several tools available for running queries in Azure Data Explorer, including Kusto.
Kusto uses a role-based access control (RBAC) model, under which authenticated principals are mapped to roles, and get access according to the roles they're assigned.
Note: Azure Data Explorer is a highly scalable and secure analytics service that enables you to do rich exploration of structured and unstructured data for instant insights. Optimized for ad-hoc queries, Azure Data Explorer enables rich data exploration over raw, structured, and semi-structured data delivering fast time to insight. Query with a modern, intuitive query language that offers fast, ad-hoc, and advanced query capabilities over high-rate data volumes and varieties
Reference:
https://docs.microsoft.com/en-us/azure/data-explorer/tools-integrations-overview

Community vote distribution
D (100%)

SriLen Highly Voted 3 years, 7 months ago
D. is the correct Answer , Azure Dashboards https://docs.microsoft.com/en-us/azure/azure-portal/azure-portal-dashboards
upvoted 47 times

saschgo 3 years, 2 months ago
Yes, Azure Dashboards can use a custom markdown tile to display custom, static content
https://docs.microsoft.com/en-us/azure/azure-portal/azure-portal-markdown-tile
upvoted 4 times

Pomphard Highly Voted 3 years, 6 months ago
A, C, and D all support visuals from Azure Monitor as well as Kusto queries and RBAC. The only answer which also supports markdown, though, is D - dashboards.
upvoted 32 times

stainz 3 years, 3 months ago
https://docs.microsoft.com/en-us/azure/devops/report/dashboards/add-markdown-to-dashboard?view=azure-devops
upvoted 2 times

saschgo 3 years, 2 months ago
That source is about Dashboards in Azure DevOps - that is out of scope with regard to given answers
https://docs.microsoft.com/en-us/azure/devops/report/dashboards/add-markdown-to-dashboard?view=azure-devops
upvoted 1 times

Spectrum128k Most Recent 10 months, 3 weeks ago
I actually think this is 'C' - Data Explorer as the MS 'learn more' page on this expressly talks about KQL as an advantage of Data Explorer whereas the similar page for 'Dashboards' doesn't mention KQL and I can't find any KQL option in the dashboards tile itself.
https://learn.microsoft.com/en-us/azure/data-explorer/
https://learn.microsoft.com/en-gb/azure/azure-portal/azure-portal-dashboards?WT.mc_id=Portal-Microsoft_Azure_PortalDashboard
upvoted 1 times

freddyneen 8 months, 3 weeks ago
You can Pin any KQL query to dashboard from Application Insights.
upvoted 1 times

flafernan 1 year, 1 month ago
C: "Consolidated monitoring strategy can be created using Azure Dashboard or Azure Data Explorer (Kusto). Azure Dashboard allows you to create custom dashboards with monitoring widgets and also supports adding formatted text using Markdown. On the other hand, Azure Data Explorer provides advanced capabilities of querying using Kusto Query Language (KQL) and getting real-time data with the latest data. Choosing between the two options will depend on the specific requirements of the project and the level of customization and analysis required."
upvoted 1 times

flafernan 1 year, 1 month ago
C: "A estratégia de monitoramento consolidado pode ser criada usando o Azure Dashboard ou o Azure Data Explorer (Kusto). O Azure Dashboard permite criar painéis personalizados com widgets de monitoramento e também suporta a adição de texto formatado usando Markdown. Por outro lado, o Azure Data Explorer fornece recursos avançados de consulta usando Kusto Query Language (KQL) e a obtenção de dados em tempo real com os dados mais recentes. A escolha entre as duas opções dependerá dos requisitos específicos do projeto e do nível de personalização e análise necessários."
upvoted 1 times

renzoku 1 year, 2 months ago
Selected Answer: D
D. Azure dashboards
Control access and permissions to the dashboard based on RBAC
Include visuals from Azure Monitor, which allows you to query and analyze data using the KQL
Can add text and documentation using markdown format
Provide real-data updating, ensuring the latest available data

Azure Monitor(Provides insights into the performance, health, and availability of your applications and resources)
Directly it doesn't support capabilities to add documentation written in markdown format.

Microsoft Power BI(Business intelligence tool that allows you to create interactive dashboards and reports)
Does not align directly with RBAC by itself.
Does not provide the same level of real-time or near-real-time data availability as Azure Monitor, Azure Dashboard.

Azure Data Explorer(Perful tool for ingesting, analyzing, and visualizing large volumes of data)
Does not align directly with RBAC by itself.
Focused on data storage, query, and analysis rather than providing a platform for documentation
upvoted 1 times

ShomaV 1 year, 3 months ago
Correct answer C
upvoted 1 times

ShomaV 1 year, 4 months ago
Answer could be C as well
Data Explorer supports basic markdown syntax. You cannot use markdown for emojis, images, and rendered markdown tables. Data Explorer renders only two levels of markdown headers.
https://learn.microsoft.com/en-us/azure/databricks/data/markdown-data-comments
upvoted 1 times

PATILDXB 1 year, 5 months ago
Azure Dashboard does not meet the following "Use the latest data available for each visual". It can only take data that is 30 min old to 30 days old. Hence, correct answer is Data Explorer.
upvoted 1 times

NK203 1 year, 5 months ago
https://learn.microsoft.com/en-us/azure/azure-portal/azure-portal-dashboards. You can choose from the past 30 minutes to the past 30 days or define a custom range.It is "You can" ,not "You only".
upvoted 2 times

mohiniu 1 year, 6 months ago

Azure Data Explorer is a desktop app to view your storage accounts locally on your desktop .
So , Azure Data Explorer cannot be correct.
upvoted 3 times

budha 1 year, 9 months ago
It was on my exam on December 7, 2022.
upvoted 4 times

meoukg 1 year, 10 months ago
I chose Azure Dashboard, appeared on my exam yesterday, I passed
upvoted 5 times

TtotheA2021 1 year, 12 months ago
Selected Answer: D
See docs microsoft regarding Azure Dashboards - custom markdown
upvoted 1 times

pkg007 2 years ago
Correct answer : C - Azure Data Explorer as it tick all the boxes
Kusto query langauge is supported in Azure Data Explorer
Mark down : https://docs.microsoft.com/en-us/azure/azure-portal/azure-portal-markdown-tile
Dash board : https://docs.microsoft.com/en-us/azure/data-explorer/azure-data-explorer-dashboards
RBAC : https://docs.microsoft.com/en-us/azure/data-explorer/kusto/management/access-control/role-based-authorization

Near real time data : https://docs.microsoft.com/en-us/azure/data-explorer/data-explorer-overview#when-should-you-use-azure-data-explorer
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: D
Azure Data Explorer and Microsoft Power BI are incorrect since these are used for Data Analytics
Azure Monitor is just the monitoring solution in Azure

Answer is D
upvoted 1 times

Govcomm 2 years, 1 month ago
Azure Dashboard
upvoted 1 times

Mcelona 2 years, 4 months ago
Selected Answer: D
Use Azure Dashboard
upvoted 2 times

Question #11 *Topic 3*

You are automating the testing process for your company.
You need to automate UI testing of a web application.
Which framework should you use?

A. JaCoco

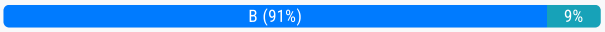
B. Selenium

C. Xamarin.UITest

D. Microsoft.CodeAnalysis

Suggested Answer: *B*
Performing user interface (UI) testing as part of the release pipeline is a great way of detecting unexpected changes, and need not be difficult. Selenium can be used to test your website during a continuous deployment release and test automation.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/test/continuous-test-selenium?view=azure-devops

Community vote distribution



azureSkies13 Highly Voted 3 years ago
Just fyi for other answers.
Jacoco is a Java code coverage tool.

Xamarin.UITest is a C# testing framework using NUnit for UI Acceptance Tests on iOS and Android apps

CodeAnalysis is a code inspection tool
upvoted 35 times

AS007 Highly Voted 4 years, 4 months ago
Correct Answer
upvoted 26 times

karl84 Most Recent 11 months, 3 weeks ago
Option B was changed to Playwright, Selenium is not exist anymore.
upvoted 5 times

yana_b 1 year, 1 month ago
Selected Answer: B
Selenium
upvoted 1 times

renzoku 1 year, 2 months ago
Selected Answer: B
B. Selenium
Open-source framework for automating web browsers, you can write automated test scripts that mimic user interactions with the web application.

Microsoft.CodeAnalysis, primarily used for static code analysis.
JaCoco, tool used to analysing the code coverage of Java applications.
Xamarin.UITest, designed for automating UI testing of mobile applications rather web applications.
upvoted 1 times

albloshi86 1 year, 7 months ago
The question was changed and Selenium was not in the option.
upvoted 4 times

ABC666 1 year, 8 months ago
Selected Answer: B
Selenium

upvoted 1 times

budha 1 year, 9 months ago

It was on my exam on December 7, 2022.

upvoted 3 times

alexax578 2 years ago

Selected Answer: B

Selenium

upvoted 1 times

larrymm 2 years, 1 month ago

At least they got this right

upvoted 2 times

syu31svc 2 years, 1 month ago

Selected Answer: B

B is correct and supported by given explanation

upvoted 1 times

Govcomm 2 years, 1 month ago

Selenium web driver

upvoted 1 times

scrilan 2 years, 2 months ago

Selected Answer: B

Of course it is Selenium

upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 1 times

adamsw 2 years, 5 months ago

Selected Answer: C

Correct

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: B

Correct

https://docs.microsoft.com/en-us/azure/devops/pipelines/test/continuous-test-selenium?view=azure-devops

upvoted 2 times

sujitwarrier11 2 years, 7 months ago

Selected Answer: B

B is the obvious answer

upvoted 1 times

Question #12 *Topic 3*

You are building an ASP.NET Core application.
You plan to create an application utilization baseline by capturing telemetry data.
You need to add code to the application to capture the telemetry data. The solution must minimize the costs of storing the telemetry data.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point

A. Add the <InitialSamplingPercentage>99</InitialSamplingPercentage> parameter to the ApplicationInsights.config file.

B. From the code of the application, enable adaptive sampling.

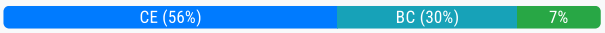
C. From the code of the application, add Azure Application Insights telemetry.

D. Add the <MaxTelemetryItemsPerSecond>5</MaxTelemetryItemsPerSecond> parameter to the ApplicationInsights.config file.

E. From the code of the application, disable adaptive sampling.

Suggested Answer: *BD*
Sampling is a feature in Azure Application Insights. It is the recommended way to reduce telemetry traffic, data costs, and storage costs, while preserving a statistically correct analysis of application data.
The Application Insights SDK for ASP.NET Core supports both fixed-rate and adaptive sampling. Adaptive sampling is enabled by default.
D: For adaptive sampling: The volume is adjusted automatically to keep within a specified maximum rate of traffic, and is controlled via the setting
MaxTelemetryItemsPerSecond. If the application produces a low amount of telemetry, such as when debugging or due to low usage, items won't be dropped by the sampling processor as long as volume is below MaxTelemetryItemsPerSecond.
Note: In ApplicationInsights.config, you can adjust several parameters in the AdaptiveSamplingTelemetryProcessor node. The figures shown are the default values:
<MaxTelemetryItemsPerSecond>5</MaxTelemetryItemsPerSecond>
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/sampling

Community vote distribution



077dammy Highly Voted 3 years, 7 months ago
Ans should be C & E.
upvoted 57 times

prashantjoge 2 years, 5 months ago
https://docs.microsoft.com/en-us/azure/azure-monitor/app/asp-net-core#enable-client-side-telemetry-for-web-applications
C & E has to be correct. Adaptive sampling is turned on by default. So we need to first enable telemetry, then use fixed-rate sampling. (see other answers for why)
upvoted 4 times

prashantjoge 2 years, 5 months ago
This is an asp.net core application, so there is no applicationinsights.config file. D is definitely incorrect
upvoted 2 times

sha1979 2 years, 1 month ago
There is I believe,
With ASP.NET Core and with Microsoft.ApplicationInsights.AspNetCore >= 2.15.0 you can configure AppInsights options via appsettings.json

In ApplicationInsights.config, you can adjust several parameters in the AdaptiveSamplingTelemetryProcessor node. The figures shown are the default values:

<MaxTelemetryItemsPerSecond>5</MaxTelemetryItemsPerSecond>

The target rate of logical operations that the adaptive algorithm aims to collect on each server host. If your web app runs on many

hosts, reduce this value so as to remain within your target rate of traffic at the Application Insights portal.
https://docs.microsoft.com/en-us/azure/azure-monitor/app/sampling
upvoted 1 times

sha1979 2 years, 1 month ago
Okay... it applied to to ASP.NET applications, not to ASP.NET Core applications. Learn about configuring adaptive sampling for ASP.NET Core applications later in this document.
upvoted 1 times

saponazureguy 3 years, 7 months ago
Correct! The keywords here are "ASP.NET core application". There is no ApplicationInsights.config file in ASP.NET Core applications (it exists only in ASP.NET) and any setting needs to be done through code itself.

Also, Adaptive sampling is enabled by default for all ASP.NET core and ASP.NET applications.

https://docs.microsoft.com/en-us/azure/azure-monitor/app/sampling
upvoted 5 times

HeyTN 2 years, 5 months ago
it's not true https://docs.microsoft.com/en-us/azure/azure-monitor/app/asp-net-core
upvoted 1 times

imanonion 1 year, 7 months ago
this article also proves that ASP.Net CORE apps do not use ApplicationInsights.config. please read it again.
upvoted 3 times

fflyin2k 3 years, 4 months ago
E is "disable adaptive sampling". it does no make sense. the question mentioned "minimize cost of storing the telemetry data", so adaptive sampling should not be disabled. And, in ASP.NET Core, adaptive sampling is enabled by default.
upvoted 17 times

Yatoom 1 year, 10 months ago
I agree, and just disabling adaptive sampling does not magically enable fixed-rate sampling.
upvoted 2 times

yana_b 1 year, 1 month ago
Although it (i.e. ingestion sampling) doesn't reduce the telemetry traffic sent from your app, it does reduce the amount processed and retained (and charged for) by Application Insights. Set the sampling rate in the Usage and estimated costs page.
Default setting is adaptive sampling, but in order to set ingestion sampling, you have to disable the adaptive sampling and set the sampling rate in the Usage and estimated costs page:
upvoted 2 times

MrMonkfish 3 years ago
C & E
Disable Adaptive Sampling and use Fixed Rate Sampling instead:
"Fixed-rate sampling reduces the volume of telemetry sent from both your ASP.NET or ASP.NET Core or Java server and from your users' browsers. You set the rate. The client and server will synchronize their sampling so that, in Search, you can navigate between related page views and requests."
https://docs.microsoft.com/en-us/azure/azure-monitor/app/sampling
upvoted 24 times

FunkyB 2 years, 4 months ago
MrMonkfish, thank you very much for providing the link. Thanks to everyone that is positive.
upvoted 4 times

agueda Highly Voted 3 years, 7 months ago
C and E
https://docs.microsoft.com/en-us/azure/azure-monitor/app/asp-net-core
upvoted 11 times

ozbonny Most Recent 6 months, 4 weeks ago
Selected Answer: CE
C and E since Adaptive sampling is already true by default in dot net core
upvoted 1 times

vsvaid 8 months, 3 weeks ago

Normally these two steps would do it in combination but second step is not there.

1) Disable Adabptive Sampling
2) Changing Usage and estimated costs->Data Sampling in Azure

upvoted 1 times

ozbonny 6 months, 4 weeks ago

maybe is not there because the 2) is in azure and the question says "in code"

upvoted 1 times

vsvaid 9 months ago

Selected Answer: CE

By disabling Adaptive Sampling, we can use the ingestion sampling. Then we can then set the sampling rate in the Usage and estimated costs.

upvoted 1 times

Joe_Mauma 1 year, 1 month ago

Selected Answer: BC

are building an ASP.NET Core application.
You plan to create an application utilization baseline by capturing telemetry data.
You need to add code to the application to capture the telemetry data. The solution must minimize the costs of storing the telemetry data.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point
A. Add the <InitialSamplingPercentage>99</InitialSamplingPercentage> parameter to the ApplicationInsights.config file.
B. From the code of the application, enable adaptive sampling.
C. From the code of the application, add Azure Application Insights telemetry. Most Voted
D. Add the <MaxTelemetryItemsPerSecond>5</MaxTelemetryItemsPerSecond> parameter to the ApplicationInsights.config file.
E. From the code of the application, disable adaptive sampling.

upvoted 2 times

varinder82 9 months, 3 weeks ago

You are 10000% wrong need to disable adaptive sampling

upvoted 1 times

ieboaix 1 year, 1 month ago

C&E.
1. Adaptive Sampling is by default which needed to be disabled. so, E is in and B is out
2.there is no ApplicationInsights.config in .NET Core app, so A and D are out.
3. C & E are the winer

upvoted 1 times

yana_b 1 year, 1 month ago

Selected Answer: CE

Ingestion sampling reduces the amount processed and retained (and charged for) by Application Insights.
Set the sampling rate in the Usage and estimated costs page.
Default setting is adaptive sampling, but in order to set ingestion sampling, you have to disable the adaptive sampling and set the sampling rate in the Usage and estimated costs page.

Source: https://learn.microsoft.com/en-us/azure/azure-monitor/app/sampling

upvoted 1 times

flafernan 1 year, 1 month ago

I hope this sheds some light on why options A, C, and E are not the best choices for minimizing telemetry data storage costs. Options B and D are the correct answers to meet telemetry capture requirements with minimal costs.

upvoted 1 times

rick1010 1 year, 3 months ago

Configure sampling settings
Use extension methods of TelemetryProcessorChainBuilder as shown below to customize sampling behavior.

Important

If you use this method to configure sampling, please make sure to set the aiOptions.EnableAdaptiveSampling property to false when calling

AddApplicationInsightsTelemetry(). After making this change, you then need to follow the instructions in the code block below exactly in order to re-enable adaptive sampling with your customizations in place. Failure to do so can result in excess data ingestion. Always test post changing sampling settings, and set an appropriate daily data cap to help control your costs.

```
builder.Services.AddApplicationInsightsTelemetry(new ApplicationInsightsServiceOptions
{
EnableAdaptiveSampling = false,
});
```

upvoted 1 times

Fal991l 1 year, 4 months ago

Selected Answer: BC

To capture telemetry data and minimize storage costs for an ASP.NET Core application, you should enable **adaptive sampling** in the code of the application and add **Azure Application Insights telemetry**[1]. Adaptive sampling ensures that only a representative sample of telemetry data is captured, reducing the overall volume of data and minimizing storage costs[3].

So, the two actions you should perform are **B. From the code of the application, enable adaptive sampling** and **C. From the code of the application, add Azure Application Insights telemetry**.

upvoted 2 times

Fal991l 1 year, 4 months ago

You can disable adaptive sampling and use fixed-rate sampling instead to reduce the volume of telemetry sent from your ASP.NET or ASP.NET Core or Java server and from your users' browsers. With fixed-rate sampling, you can set the rate and the client and server will synchronize their sampling so that you can navigate between related page views and requests in Search .

upvoted 1 times

Fal991l 1 year, 4 months ago

The best answer to the question "You are building an ASP.NET Core application. You plan to create an application utilization baseline by capturing telemetry data. You need to add code to the application to capture the telemetry data. The solution must minimize the costs of storing the telemetry data." would be **B. From the code of the application, enable adaptive sampling**.

Adaptive sampling is a feature in Application Insights that reduces telemetry traffic and storage costs while preserving a statistically correct analysis of application data. It ensures that only a representative sample of telemetry data is captured, reducing the overall volume of data and minimizing storage costs.

Option E, "From the code of the application, disable adaptive sampling," would not help minimize the costs of storing telemetry data.

upvoted 2 times

col2511kol 1 year, 5 months ago

Selected Answer: CE

If your goal is to minimize the cost of storing telemetry data, using Fixed Rate Sampling is a more appropriate approach. In this case, the correct answers would be:

C. From the code of the application, add Azure Application Insights telemetry.
E. From the code of the application, disable adaptive sampling.

By disabling adaptive sampling (E) and using Fixed Rate Sampling, you can control the volume of telemetry data sent from your application, reducing the storage cost. Adding Azure Application Insights telemetry (C) will enable you to collect and analyze the telemetry data from your ASP.NET Core application.

upvoted 4 times

jimmyyml 1 year, 6 months ago

Selected Answer: BC

B. From the code of the application, enable adaptive sampling.
C. From the code of the application, add Azure Application Insights telemetry.

Explanation:
To capture telemetry data and minimize storage costs, you should enable adaptive sampling in the code of the application and add Azure Application Insights telemetry. Adaptive sampling ensures that only a representative sample of telemetry data is captured, reducing the overall volume of data and minimizing storage costs. Adding Azure Application Insights telemetry to the code allows the application to send telemetry data to the Application Insights service. The other options listed are not relevant to capturing telemetry data and minimizing storage costs.

upvoted 2 times

budha 1 year, 9 months ago

It was on my exam on December 7, 2022.

upvoted 2 times

Atos 2 years ago

Process of elimination would suggest B&E.

Not A: You would not add, but modify the parameter, but reducing to 99 would seem trivial. Also, as i understand there's no ApplicationInsights.config for
ASP.NET Core applications.

Not B: Adaptive sampling is default

Not D: Adding the parameter: <MaxTelemetryItemsPerSecond>5</MaxTelemetryItemsPerSecond>, would be pointless as by default this is in place. Also, as i understand there's no ApplicationInsights.config for ASP.NET Core applications.

upvoted 1 times

hip9k 2 years, 1 month ago

Selected Answer: CD

As "minimize the cost" is specified as requirement I would say it will be CD
Adaptive sampling is ON by default which is good + we can lower amount of logs even more by MaxTelemetryItemsPerSecond parameter

upvoted 2 times

AntonyLejoS 2 years, 1 month ago

Selected Answer: BD

We need to enable sampling also should ensure minimum data is sampled. so given answer is correct

upvoted 2 times

Question #13 *Topic 3*

You have an Azure DevOps organization named Contoso and an Azure subscription. The subscription contains an Azure virtual machine scale set named VMSS1 and an Azure Standard Load Balancer named LB1. LB1 distributes incoming requests across VMSS1 instances.
You use Azure DevOps to build a web app named App1 and deploy App1 to VMSS1. App1 is accessible via HTTPS only and configured to require mutual authentication by using a client certificate.
You need to recommend a solution for implementing a health check of App1. The solution must meet the following requirements:
➪ Identify whether individual instances of VMSS1 are eligible for an upgrade operation.
➪ Minimize administrative effort.
What should you include in the recommendation?

A. an Azure Load Balancer health probe

B. Azure Monitor autoscale

C. the Custom Script Extension

D. the Application Health extension

Suggested Answer: *D*
Monitoring your application health is an important signal for managing and upgrading your deployment. Azure virtual machine scale sets provide support for rolling upgrades including automatic OS-image upgrades, which rely on health monitoring of the individual instances to upgrade your deployment. You can also use health extension to monitor the application health of each instance in your scale set and perform instance repairs using automatic instance repairs.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-health-extension

Community vote distribution
D (100%)

SriLen Highly Voted 3 years, 7 months ago
D. the Application Health extension -- is correct
upvoted 21 times

vsvaid Most Recent 9 months ago
Selected Answer: D
Application Health Extension
upvoted 1 times

flafernan 1 year, 1 month ago
D: For the use of VM Scale Set, using load balance via code within your build of a web app in Azure DevOps for example, the “Application Health extension” is used, which will play the role similar to a Load Balancer Health probe within the portal. This extension used in your code checks the response of a Vm Scale Set sizing instance. When one of the instances to be scheduled does not respond through the configured TCP port, it will have the status of Unhealthy. If you need an autoscale and it doesn't respond, this extension can perform automatic repairs for that instance. Example JSON code from a REST API. It also runs on Azure PowerShell and Azure CLI 2.0.
upvoted 1 times

RonZhong 1 year, 4 months ago
D. the Application Health extension

When to use the Application Health extension
The Application Health Extension is deployed inside a Virtual Machine Scale Set instance and reports on application health from inside the scale set instance. The extension probes on a local application endpoint and will update the health status based on TCP/HTTP(S) responses received from the application. This health status is used by Azure to initiate repairs on unhealthy instances and to determine if an instance is eligible for upgrade operations.

The extension reports health from within a VM and can be used in situations where an external probe such as the Azure Load Balancer health probes can’t be used.

https://learn.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-health-extension?tabs=rest-api

upvoted 1 times

RealRaymond 1 year, 5 months ago

D. https://learn.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-health-extension?tabs=rest-api#when-to-use-the-application-health-extension

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: D

D is correct as supported by given explanation

upvoted 2 times

Govcomm 2 years, 1 month ago

D. The application health extension

upvoted 1 times

Mcelona 2 years, 4 months ago

Selected Answer: D

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-custom-probe-overview

Inside Limitations section you find the right answer.

upvoted 4 times

nqthien041292 2 years, 5 months ago

Selected Answer: D

Vote D

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: D

correct

upvoted 1 times

lugospod 2 years, 7 months ago

Got this January 2022

upvoted 3 times

Pankaj78 2 years, 9 months ago

Selected Answer: D

Application Health extension

upvoted 3 times

saschgo 3 years, 2 months ago

Why answer 'A' is not correct? I recently used an existing Load Balancer Health Probe, an external health probe in contrast to an internal health probe like Application Health extension, to provide health checks required for 'rolling' upgrade policy and 'automatic instance repairs'.

https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-health-extension#when-to-use-the-application-health-extension

upvoted 2 times

ChauPhan 2 years, 10 months ago

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-custom-probe-overview

upvoted 1 times

nicksu 3 years, 2 months ago

I would say, that LB health probe doesn't support mutual authentication with client certificate

upvoted 6 times

ChauPhan 2 years, 10 months ago

Limitations

HTTPS probes do not support mutual authentication with a client certificate.

You should assume Health probes will fail when TCP timestamps are enabled.

A basic SKU load balancer health probe isn't supported with a virtual machine scale set.

upvoted 6 times

TanmoyD 3 years, 4 months ago

D is the correct answer.

upvoted 1 times

PengPai6 3 years, 4 months ago

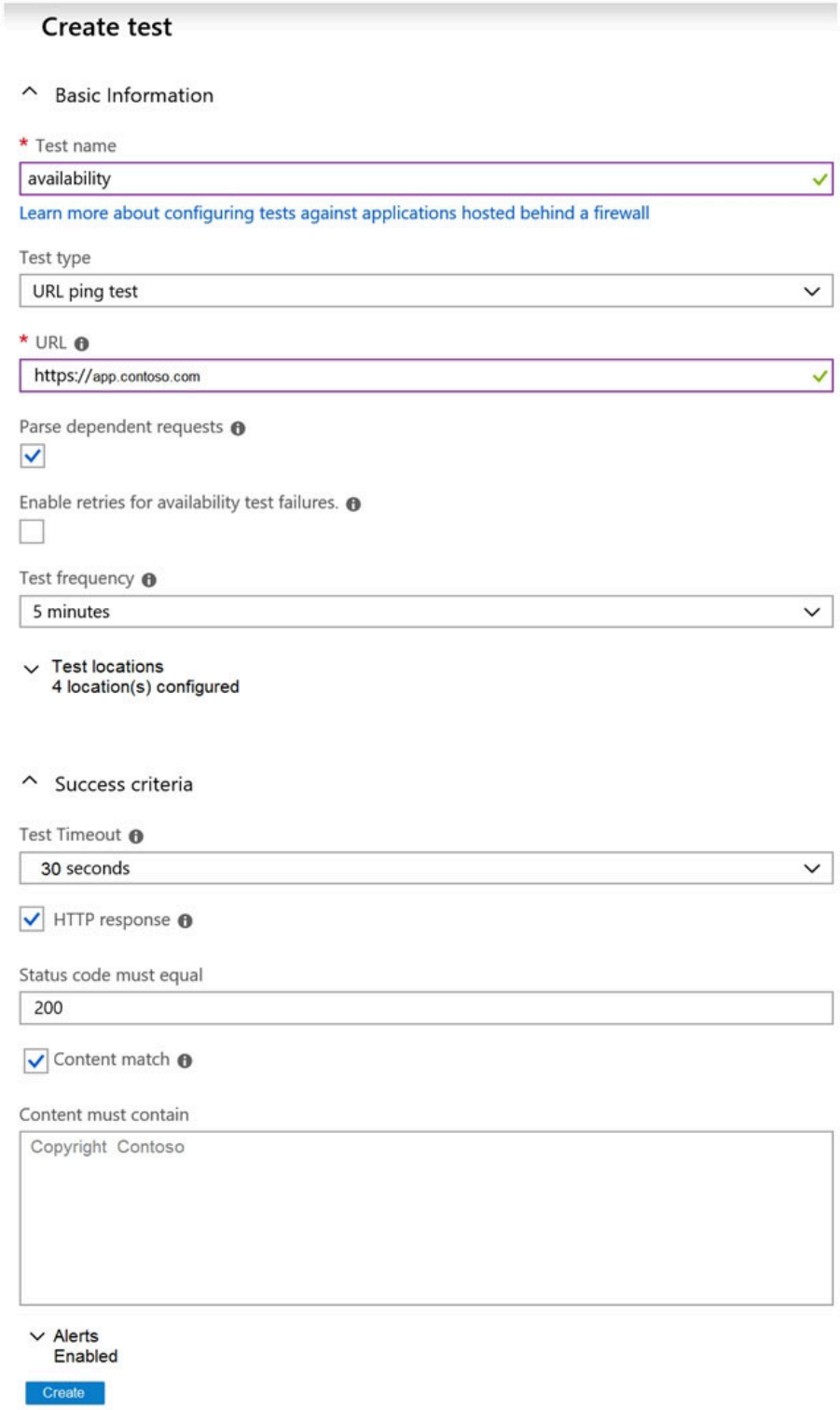
correct Ans

upvoted 2 times

HOTSPOT -

You have an application named App1 that has a custom domain of app.contoso.com.

You create a test in Azure Application Insights as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The test will execute **[answer choice]**.

- every 30 seconds at a random location
- every 30 seconds per location
- every five minutes at a random location
- every five minutes per location

The test will pass if **[answer choice]** within 30 seconds.

- App1 responds to an ICMP ping
- the HTML of App1 and the HTML from URLs in <a> tags load
- all the HTML, JavaScripts, and images of App1 load

Suggested Answer:

Answer Area

The test will execute **[answer choice]**.

- every 30 seconds at a random location
- every 30 seconds per location
- every five minutes at a random location
- every five minutes per location

The test will pass if **[answer choice]** within 30 seconds.

- App1 responds to an ICMP ping
- the HTML of App1 and the HTML from URLs in <a> tags load
- all the HTML, JavaScripts, and images of App1 load

Box 1: every five minutes at a random location

Test frequency: Sets how often the test is run from each test location. With a default frequency of five minutes and five test locations, your site is tested on average every minute.

Box 2:

Parse dependent requests: Test requests images, scripts, style files, and other files that are part of the web page under test. The recorded response time includes the time taken to get these files. The test fails if any of these resources cannot be successfully downloaded within the timeout for the whole test.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/app/monitor-web-app-availability

Tesshu Highly Voted 3 years, 5 months ago

I believe the first one should be "every five minutes per location" since "every five minutes at a random location" means that every five minutes only 1 location would send the request and that is wrong.

upvoted 81 times

rdemontis 2 years, 5 months ago

It says "from each test location". If would be random you wouldn't have the certainty to each location every 5 minutes. It could be happen that a location would be test twice and another one zero.

upvoted 6 times

LeeVee 3 years, 5 months ago

and 2nd answer should be App1 responds to ICMP

upvoted 10 times

Sylph 3 years, 5 months ago

The name "URL ping test" is a bit of a misnomer. To be clear, this test is not making any use of ICMP (Internet Control Message Protocol) to check your site's availability. Instead it uses more advanced HTTP request functionality to validate whether an endpoint is responding.

https://docs.microsoft.com/en-us/azure/azure-monitor/app/monitor-web-app-availability#create-a-url-ping-test

upvoted 22 times

Tesshu 3 years, 5 months ago
Right, second answer is correct, it is all HTML since "parse dependant requests" is checked.
upvoted 15 times

Leandrocei 2 years, 2 months ago
Correct I believe the first one should be "every five minutes per location". Came today 22 july 9
upvoted 8 times

CheesusCrust89 3 years, 2 months ago
answer one is also correct, see https://docs.microsoft.com/en-us/azure/azure-monitor/app/availability-multistep#frequency--location
upvoted 5 times

binhdortmund 1 year, 8 months ago
From your URL:
Sets how often the test is run from --> EACH <-- test location. With a default frequency of five minutes and five test locations, your site is tested on average every minute.

So it must be "every 5mins per location"
upvoted 8 times

sheva370 Highly Voted 3 years, 1 month ago
Box1: every five minutes per location
I tested this in my lab and confirmed that each location will be tested every minute.

Box2: All the HTML, JavaScripts, and images of App1 load
If you selected Parse dependent requests, then all the images, style files, scripts, and other dependent resources must have been received within this period.

https://docs.microsoft.com/en-us/azure/azure-monitor/app/monitor-web-app-availability
upvoted 81 times

jvyas 2 years, 3 months ago
Thank you for the link. This confirms the answers from the above link.
"This setting determines how often the test is run from each test location. With a default frequency of five minutes and five test locations, your site is tested every minute on average."
upvoted 2 times

ozbonny Most Recent 6 months, 4 weeks ago
per location and all I think
upvoted 2 times

vsvaid 9 months ago
1st box- every 5mins per location
2nd Box: Since the parse option is enables, all data (file, html, js code) should be loaded. Option 3 in second box
upvoted 2 times

Pamban 1 year, 3 months ago
1st option should be every five minutes per location

Test frequency --- Sets how often the test is run from each test location. With a default frequency of five minutes and five test locations, your site is tested on average every minute

Source: https://learn.microsoft.com/en-us/previous-versions/azure/azure-monitor/app/availability-multistep#frequency--location
upvoted 2 times

SowmSan 1 year, 5 months ago
Which one is the Correct answer?
upvoted 1 times

Fal991l 1 year, 5 months ago
GTP:
Based on the provided exhibit, the test in Azure Application Insights will execute every 30 seconds per location, meaning that the test will run once every 30 seconds at each of the selected locations. Therefore, the correct answer is option B.

Regarding the success criteria, the test will pass if the HTML of App1 and the HTML from URLs in <a> tags load successfully. This means that the test will check for the availability and accessibility of the web page content, and not for the availability of the server or the network connection. Therefore, the correct answer is option B.

Regarding the Parse dependent requests option, if this option is enabled, the test will also check for the successful loading of all the dependent resources (such as images, JavaScript files, and CSS files) required to render the web page. This can provide more comprehensive information about the performance and availability of the web page. However, it may also increase the test duration and the data size. Therefore, it depends on the specific requirements and constraints of the testing scenario.

upvoted 1 times

syu31svc 2 years, 1 month ago

https://docs.microsoft.com/en-us/azure/azure-monitor/app/monitor-web-app-availability

"Parse dependent requests The test requests images, scripts, style files, and other files that are part of the webpage under test. The recorded response time includes the time taken to get these files. The test fails if any of these resources can't be successfully downloaded within the timeout for the whole test. If the option is not enabled, the test only requests the file at the URL that you specified. Enabling this option results in a stricter check. The test might fail for cases that aren't noticeable from manually browsing through the site."

2nd dropdown is correct

upvoted 1 times

syu31svc 2 years, 1 month ago

As for the first dropdown, it is every 5 mins per location. I don't see how only 1 location is being configured

upvoted 1 times

Govcomm 2 years, 1 month ago

Every 5 minutes per location

Parse dependency: Load all

upvoted 1 times

Cheehp 2 years, 5 months ago

Selected during exam.

Box1: every five minutes at a random location

Box2: All the HTML, JavaScripts, and images of App1 load

upvoted 3 times

Pankaj78 2 years, 9 months ago

"every five minutes per location" should be the answer ,sending request to random location means some location may get chance to get tested twice or more which is not the case when you have 5 tests/5 minutes= 1 test /1 minute

upvoted 2 times

rdemontis 2 years, 5 months ago

I agree with you

upvoted 2 times

photon99 2 years, 9 months ago

This is called as synthetic monitoring. And it MUST run from ALL 5 locations not just any random location.

upvoted 1 times

rajvelm 2 years, 10 months ago

Came in today 7 Nov 2021

upvoted 3 times

ziizai 3 years ago

Tested in lab by using default 5 mins and 5 locations. Every location is tested every 5 mins, although the tests don't happen at the same time. The tests happen in turn, like location1 -> location2 -> location3 -> location4 -> location5 -> location1 -> location2 -> location3 -> location4 -> location5

upvoted 6 times

ziizai 3 years ago

tested in lab, using default 5 min and 5 locations. Every location is tested every 5 minutes, although the tests for all 5 locations doesn't happen at the same time.

upvoted 2 times

ukkuru 3 years, 1 month ago

The second one should be the last option: https://docs.microsoft.com/en-us/azure/azure-monitor/app/monitor-web-app-availability : Test requests images, scripts, style files, and other files that are part of the web page under test

upvoted 1 times

ScreamingHand 3 years, 2 months ago

Parse dependent requests:

Test requests images, scripts, style files, and other files that are part of the web page under test. The recorded response time includes the time taken to get these files. The test fails if any of these resources cannot be successfully downloaded within the timeout for the whole test. If the option is not checked, the test only requests the file at the URL you specified. Enabling this option results in a stricter check. The test could fail for cases, which may not be noticeable when manually browsing the site.

upvoted 1 times

Question #15 *Topic 3*

You have a build pipeline in Azure Pipelines that occasionally fails.
You discover that a test measuring the response time of an API endpoint causes the failures.
You need to prevent the build pipeline from failing due to the test.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Set Flaky test detection to Off.

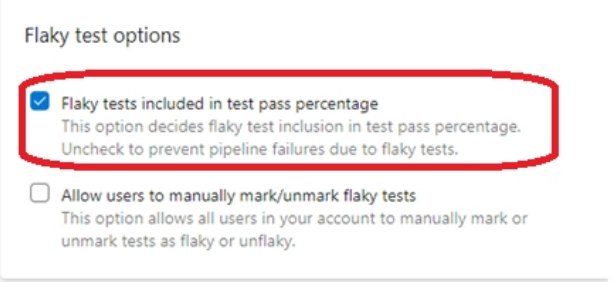
B. Clear Flaky tests included in test pass percentage.

C. Enable Test Impact Analysis (TIA).

D. Manually mark the test as flaky.

E. Enable test slicing.

Suggested Answer: *BD*
D: You can mark or unmark a test as flaky based on analysis or context, by choosing Flaky.
To configure flaky test management, choose Project settings, and select Test management in the Pipelines section.
B:
Slide the On/Off button to On.



Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/test/flaky-test-management

Community vote distribution
BD (100%)

nvnrao57 Highly Voted 3 years, 4 months ago
Given ans is correct
upvoted 12 times

vxl 1 year, 7 months ago
Came up in my exam (febr 2023)
upvoted 5 times

zellck Highly Voted 1 year, 3 months ago
Selected Answer: BD
BD is the answer.

https://learn.microsoft.com/en-us/azure/devops/pipelines/test/flaky-test-management?view=azure-devops#flaky-test-management-and-reporting
On the Test management page under Flaky test options, you can set options for how flaky tests are included in the Test Summary report. Flaky test data for both passed and failed test is available in Test results. The Flaky tag helps you identify flaky tests. By default, flaky tests are included in the Test Summary. However, if you want to ensure flaky test failures don't fail your pipeline, you can choose to not include them in your test summary and suppress the test failure. This option ensures flaky tests (both passed and failed) are removed from the pass percentage and shown in Tests not reported.
upvoted 5 times

zellck 1 year, 3 months ago
https://learn.microsoft.com/en-us/azure/devops/pipelines/test/flaky-test-management?view=azure-devops#tests-marked-as-flaky
You can mark or unmark a test as flaky based on analysis or context, by choosing Flaky (or UnFlaky, depending on whether the test is already marked as flaky.)
upvoted 4 times

sondrex Most Recent 2 months, 1 week ago
every five minutes per location
all the HTML, JavaScripts, and images of App1 load
upvoted 1 times

vsvaid 9 months ago
Selected Answer: BD
Agree with the answer
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: BD
Correct answers are B & D
upvoted 2 times

AlexeyG 1 year, 6 months ago
got this in 02 March 2023 exams. scored 870 marks.
upvoted 4 times

Racheal28 1 year, 9 months ago
Go this on my exam today and selected B , D .Passed
upvoted 2 times

budha 1 year, 9 months ago
It was on my exam on December 7, 2022.
upvoted 3 times

syu31svc 2 years, 1 month ago
Selected Answer: BD
Given answers are supported by explanation

B and D
upvoted 2 times

Govcomm 2 years, 1 month ago
Mark Flaky test and clear the Flaky test
upvoted 1 times

Mcelona 2 years, 4 months ago
Selected Answer: BD
Check https://docs.microsoft.com/en-us/azure/devops/pipelines/test/flaky-test-management ==> B & D is the right answer
upvoted 1 times

rdemontis 2 years, 6 months ago
Selected Answer: BD
correct
upvoted 2 times

Pankaj78 2 years, 9 months ago
Selected Answer: BD
correct
upvoted 1 times

debanjan10 2 years, 9 months ago
Selected Answer: BD
B and D
upvoted 1 times

Varun1980 3 years, 4 months ago
why is it not A?
upvoted 1 times

mpindado 3 years, 3 months ago
If you disable flaky test detection, then when the test fails the pipeline is always going to be marked as failed. With flaky tests detection AZ can detect the failed test is flaky and let the pipeline finishes ok.
upvoted 8 times

Question #16 *Topic 3*

Your company hosts a web application in Azure. The company uses Azure Pipelines for the build and release management of the application. Stakeholders report that the past few releases have negatively affected system performance.
You configure alerts in Azure Monitor.
You need to ensure that new releases are only deployed to production if the releases meet defined performance baseline criteria in the staging environment first.
What should you use to prevent the deployment of releases that fall to meet the performance baseline?

A. an Azure Scheduler job

B. a trigger

C. a gate

D. an Azure function

Suggested Answer: *C*
Scenarios and use cases for gates include:
➪ Quality validation. Query metrics from tests on the build artifacts such as pass rate or code coverage and deploy only if they are within required thresholds.
Use Quality Gates to integrate monitoring into your pre-deployment or post-deployment. This ensures that you are meeting the key health/performance metrics
(KPIs) as your applications move from dev to production and any differences in the infrastructure environment or scale is not negatively impacting your KPIs.
Note: Gates allow automatic collection of health signals from external services, and then promote the release when all the signals are successful at the same time or stop the deployment on timeout. Typically, gates are used in connection with incident management, problem management, change management, monitoring, and external approval systems.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/continuous-monitoring https://docs.microsoft.com/en-us/azure/devops/pipelines/release/approvals/gates?view=azure-devops

Community vote distribution

C (100%)

27close Highly Voted 3 years, 10 months ago
a gate
upvoted 19 times

Jkmr622 Highly Voted 3 years, 8 months ago
Si correctamundo
Dude
upvoted 8 times

ozbonny Most Recent 6 months, 4 weeks ago
Selected Answer: C
IMHO: C
upvoted 1 times

vsvaid 9 months ago
Gate check
upvoted 1 times

WH16 1 year ago
Selected Answer: C
On exam 2023-09-06, selected C. a gate
Score 933
upvoted 2 times

yana_b 1 year, 1 month ago
Selected Answer: C
configure a gate

upvoted 1 times

zellck 1 year, 3 months ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/devops/pipelines/release/approvals/gates?view=azure-devops
Gates allow automatic collection of health signals from external services and then promote the release when all the signals are successful or stop the deployment on timeout. Typically, gates are used in connection with incident management, problem management, change management, monitoring, and external approval systems.

upvoted 2 times

surensaluka 1 year, 7 months ago

Selected Answer: C

This came today for my exam on 2023-02-14.

upvoted 4 times

Marge_Simpson 1 year, 7 months ago

Selected Answer: C

The Gate!

upvoted 1 times

rikininetysix 1 year, 8 months ago

Selected Answer: C

Use a Release gate - https://learn.microsoft.com/en-us/azure/devops/pipelines/release/approvals/gates?view=azure-devops

upvoted 1 times

meoukg 1 year, 10 months ago

a gate was my answer yesterday when I sat on this exam

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: C

101% is C

upvoted 1 times

Govcomm 2 years, 1 month ago

Gate for controlling the quality.

upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: C

correct answer

upvoted 1 times

shermin1 2 years, 6 months ago

Came in exam march 13....

upvoted 2 times

RajatSahani 2 years, 9 months ago

Release Gate

upvoted 1 times

Question #17 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You manage a project in Azure DevOps.
You need to prevent the configuration of the project from changing over time.
Solution: Perform a Subscription Health scan when packages are created.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Instead implement Continuous Assurance for the project.
Note: The Subscription Security health check features in AzSK contains a set of scripts that examines a subscription and flags off security issues, misconfigurations or obsolete artifacts/settings which can put your subscription at higher risk.
Reference:
https://azsk.azurewebsites.net/04-Continous-Assurance/Readme.html

Community vote distribution
B (100%)

somnathpate Highly Voted 3 years, 4 months ago
Ans is correct!
upvoted 6 times

ozbonny Most Recent 6 months, 4 weeks ago
Selected Answer: B
Correct is B
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: B
Correct answer is no
upvoted 1 times

BlueYeti998 1 year, 8 months ago
"Secure DevOps Kit for Azure (AzSK) is being sunset". Some of the tools that will phase out seem to be ARM Checker, DevOps Kit CICD Extension and AAD Scanner (AzSK.AAD).

The tool that will replace them is Azure Tenant Security Solution (AzTS). Based on the original note, ADO Scanner - used to secure your Azure DevOps set-up will continue to be updated.

If you are looking for ARM template validation and verification only you can also check the following approaches:

Test-AzDeployment
What-if operation
Validate templates
So, if you have a dependency on Secure DevOps Kit for Azure (AzSK) make sure the update, there are options available.

DevSecOps in Azure Reference architecture is available here.
https://github.com/azsk/AzTS-docs
https://learn.microsoft.com/en-us/azure/architecture/solution-ideas/articles/devsecops-in-azure
upvoted 3 times

Samu74 1 year, 9 months ago

Probably no longer relevant because DevOps Kit (AzSK) is being sunset by end of FY21.
https://github.com/azsk/DevOpsKit-docs/blob/master/04-Continous-Assurance/Readme.md
upvoted 3 times

syu31svc 2 years, 1 month ago

Selected Answer: B

No is the answer for sure
upvoted 1 times

Govcomm 2 years, 1 month ago

Continuous Assurance
upvoted 1 times

Cheehp 2 years, 5 months ago

Selected during exam.
No.
upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: B

correct
upvoted 1 times

V_Ramon 3 years, 1 month ago

this question came today, July 28, 2021
upvoted 2 times

igorole 3 years, 2 months ago

Is this still relevant?
upvoted 4 times

Question #18 *Topic 3*

Your company uses the following resources:
✑ Windows Server 2019 container images hosted in an Azure Container Registry.
✑ Azure virtual machines that run the latest version of Ubuntu
✑ An Azure Log Analytics workspace
✑ Azure Active Directory (Azure AD)
✑ An Azure key vault
For which two resources can you receive vulnerability assessments in Azure Security Center? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. the Azure Log Analytics workspace

B. the Azure key vault

C. the Azure virtual machines that run the latest version of Ubuntu

D. Azure Active Directory (Azure AD)

E. The Windows Server 2019 container images hosted in the Azure Container Registry.

Suggested Answer: *BC*
B: Azure Security Center includes Azure-native, advanced threat protection for Azure Key Vault, providing an additional layer of security intelligence.
C: When Security Center discovers a connected VM without a vulnerability assessment solution deployed, it provides the security recommendation "A vulnerability assessment solution should be enabled on your virtual machines".
Ubuntu supported versions: 12.04 LTS, 14.04 LTS, 15.x, 16.04 LTS, 18.04 LTS
Reference:
https://docs.microsoft.com/en-us/azure/security-center/deploy-vulnerability-assessment-vm

Community vote distribution
CE (91%) 9%

dollarpo7 Highly Voted 3 years, 10 months ago
https://docs.microsoft.com/en-us/azure/security-center/features-paas
C and E
upvoted 42 times

vxl 1 year, 7 months ago
I had it in my exam (febr 2023)
upvoted 7 times

mikk 1 year, 5 months ago
did you also receive any simulation questions in exam?
upvoted 10 times

Albelev 3 years, 4 months ago
B, C are correct (KeyVault and VM). Windows container images are not supported , only Linux.
https://docs.microsoft.com/en-us/azure/security-center/defender-for-container-registries-introduction
upvoted 16 times

warchoon 1 year, 9 months ago
https://learn.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-vm
"The Microsoft Defender for Cloud vulnerability assessment extension (powered by Qualys), like other extensions, runs on top of the Azure Virtual Machine agent. So it runs as Local Host on Windows, and Root on Linux."
upvoted 1 times

ChauPhan 2 years, 10 months ago
But your link is also correct, so I don't know
Supported registries and images: Linux images in ACR registries accessible from the public internet with shell access
ACR registries protected with Azure Private Link

upvoted 1 times

ChauPhan 2 years, 10 months ago

Check carefully the above link

Service Recommendations (Free) Security alerts Vulnerability assessment

Azure Key Vault belongs to Recommendation and Security Alerts, not Vulnerability assessment

Per my personal opinion, Vulnerability assessment is usually for VMs and Image, not for Vault.

upvoted 6 times

Quirkafleeg 2 years, 9 months ago

https://docs.microsoft.com/en-us/security/benchmark/azure/security-control-vulnerability-management

Section 5.1:

"Follow recommendations from Azure Security Center on performing vulnerability assessments on your Azure virtual machines, container images, and SQL servers."

upvoted 5 times

piyipo3349 Highly Voted 3 years, 8 months ago

Answer: B & C

I know, it's weird to agree with the solution provided by exam topics. But why do I agree?

1) create a Keyvault and a VM

2) go to each resource, and search for "security" in the left pane

3) view the security recommendations. Also, note the blue banner on top stating:

"Visit Security Center to manage security across your virtual networks, data, apps, and more"

upvoted 14 times

Kalaisuran Most Recent 5 months, 2 weeks ago

Selected Answer: CE

https://learn.microsoft.com/en-us/security/benchmark/azure/security-control-vulnerability-management

Follow recommendations from Azure Security Center on performing vulnerability assessments on your Azure virtual machines, container images, and SQL servers.

upvoted 2 times

vsvaid 8 months, 3 weeks ago

Selected Answer: CE

As per

https://learn.microsoft.com/en-us/azure/defender-for-cloud/support-matrix-defender-for-cloud

upvoted 1 times

vsvaid 9 months ago

Selected Answer: CE

C and E

upvoted 1 times

gabo 11 months, 3 weeks ago

As per : https://learn.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-vm

The Vulnerability scanning is only available for virtual machines, Azure SQL databases and ACR images, so the right answer should be C, E

upvoted 3 times

WH16 1 year ago

Selected Answer: CE

On exam 2023-09-06, selected C and E

Score 933

upvoted 5 times

krzychu3000 1 year, 1 month ago

Selected Answer: CE

should be C and E

upvoted 3 times

yana_b 1 year, 1 month ago

Selected Answer: CE

Correct answer is C&E

upvoted 1 times

flafernan 1 year, 1 month ago

B,C and E. The question was poorly worded and there are 3 possible options. Azure Security Center will always look for vulnerabilities in VM (Windows/Linux) and Azure key vault. There is a particular issue regarding the Azure Security Center performing vulnerability assessments on the Azure Container Registry or on images hosted there. In fact, the search for vulnerabilities will occur in the Azure Container Registry as a whole, that is, in the service itself, in the images, in the cluster, nodes and Kubernetes pods.

upvoted 2 times

zellck 1 year, 3 months ago

Selected Answer: CE

CE is the answer.

https://learn.microsoft.com/en-us/security/benchmark/azure/security-control-vulnerability-management#51-run-automated-vulnerability-scanning-tools

Follow recommendations from Azure Security Center on performing vulnerability assessments on your Azure virtual machines, container images, and SQL servers.

upvoted 7 times

ShomaV 1 year, 4 months ago

From chatGPT

In Azure Security Center, you can receive vulnerability assessments for various resources. Some of the resources for which you can receive vulnerability assessments include:

Virtual Machines, Azure App Service,Azure Kubernetes Service (AKS), Azure SQL Database,
Azure Functions, Azure Container Registry and Azure Storage accounts.

So Answer is C&E

upvoted 1 times

Ravindu 1 year, 4 months ago

correct answers C & E

upvoted 2 times

RealRaymond 1 year, 5 months ago

C,E

https://learn.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-defender-vulnerability-management

https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-vulnerability-assessment-azure

upvoted 1 times

ParkXD 1 year, 6 months ago

From ChatGPT:

C. the Azure virtual machines that run the latest version of Ubuntu

E. The Windows Server 2019 container images hosted in the Azure Container Registry.

Azure Security Center provides vulnerability assessment for a range of resources, including virtual machines, containers, and container registries.

upvoted 2 times

Rams_84zO6n 1 year, 6 months ago

Selected Answer: BC

The given answer is correct. https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction#protect-cloud-workloads

upvoted 1 times

AlexeyG 1 year, 6 months ago

got this in 02 March 2023 exams. scored 870 marks.

upvoted 2 times

CellCS 1 year, 6 months ago

Hi @AlexyG, would you mind give us suggestion to prepare this exam, thanks

upvoted 1 times

Question #19 *Topic 3*

You use Azure Pipelines to manage build pipelines, GitHub to store source code, and Dependabot to manage dependencies.
You have an app named App1.
Dependabot detects a dependency in App1 that requires an update.
What should you do first to apply the update?

A. Create a pull request.

B. Approve the pull request.

C. Create a branch.

D. Perform a commit.

Suggested Answer: *B*
DependaBot is a useful tool to regularly check for dependency updates. By helping to keep your project up to date, DependaBot can reduce technical debt and immediately apply security vulnerabilities when patches are released. How does DependaBot work?
1. DependaBot regularly checks dependencies for updates
2. If an update is found, DependaBot creates a new branch with this upgrade and Pull Request for approval
3. You review the new Pull Request, ensure the tests passed, review the code, and decide if you can merge the change
Reference:
https://samlearnsazure.blog/2019/12/20/github-using-dependabot/

Community vote distribution
B (100%)

kumardeb Highly Voted 3 years, 10 months ago
B. Approve the pull request.
upvoted 34 times

kumardeb Highly Voted 3 years, 10 months ago
If a dependency update is found, a new Pull Request is created with the upgraded dependency and an email notification is sent. All we need to do is review the Pull Request, ensure all of the tests passed successfully, and we can confidently approve and merge this update.
upvoted 25 times

vsvaid Most Recent 9 months ago
Selected Answer: B
agree with the suggested answer
upvoted 2 times

yana_b 1 year, 1 month ago
Selected Answer: B
Approve the pull request as the rest is completed from the dependabot itself - it creates a new branch and a pull request
upvoted 1 times

zellck 1 year, 3 months ago
Gotten this in Jun 2023 exam.
upvoted 6 times

syu31svc 2 years, 1 month ago
Selected Answer: B
B is correct; just approve once depandabot "creates a new branch" and "Pull Request for approval"
upvoted 1 times

hebertpena88 2 years, 1 month ago
Selected Answer: B
Dependabot will create a new PR, just need to approve it
upvoted 2 times

Govcomm 2 years, 1 month ago
Approve the full request
upvoted 1 times

UnknowMan 2 years, 4 months ago
B. Approve the pull request.

Because dependabot automatically create a branch and a pull request for us
upvoted 2 times

Cheehp 2 years, 5 months ago
Selected during exam.
B. Approve the pull request.
upvoted 1 times

rdemontis 2 years, 6 months ago
Selected Answer: B
Correct answer as for documentation attached
upvoted 1 times

nvnrao57 3 years, 4 months ago
A. Create a pull request. - is correct
upvoted 2 times

dba7x 3 years, 3 months ago
Wrong, read the doc and you will see that Dependabot will create that PR.
upvoted 6 times

nvnrao57 3 years, 4 months ago
Correct Answer is > A. Pull Request
upvoted 2 times

idr1s 3 years, 7 months ago
Correct Answer to Review and Approve Pull Request

1) Dependabot checks for updates
2) Dependabot opens pull requests
3) You review and merge

https://dependabot.com/
upvoted 5 times

MohamedBMW 3 years, 8 months ago
A. Create Pull Request
upvoted 3 times

tom999 3 years, 8 months ago
No. Dependabot will create the pull request. We only have to approve it.
upvoted 6 times

27close 3 years, 10 months ago
agree with the solution
upvoted 3 times

Question #20 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You manage a project in Azure DevOps.
You need to prevent the configuration of the project from changing over time.
Solution: Add a code coverage step to the build pipelines.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Instead implement Continuous Assurance for the project.
Reference:
https://azsk.azurewebsites.net/04-Continous-Assurance/Readme.html

Community vote distribution
B (100%)

Alexevansigg Highly Voted 3 years, 11 months ago
No - Code Coverage is only checking how much of your code base as testscases applied to it.
upvoted 16 times

ozbonny Most Recent 6 months, 4 weeks ago
Selected Answer: B
Correct: No
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: B
correct
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: B
Code coverage is a software testing metric that determines the number of lines of code that is successfully validated under a test procedure

Answer is No
upvoted 3 times

Govcomm 2 years, 1 month ago
Continuous Assurance
upvoted 1 times

Cheehp 2 years, 5 months ago
Selected during exam.
No.
upvoted 1 times

rdemontis 2 years, 6 months ago
Selected Answer: B
correct
upvoted 1 times

V_Ramon 3 years, 1 month ago
this question came out today, July 28, 2021
upvoted 4 times

Question #21 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You manage a project in Azure DevOps.
You need to prevent the configuration of the project from changing over time.
Solution: Implement Continuous Integration for the project.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Instead implement Continuous Assurance for the project.
Reference:
https://azsk.azurewebsites.net/04-Continous-Assurance/Readme.html

Community vote distribution
B (100%)

roydeen Highly Voted 3 years, 9 months ago
CI has nothing to do with it, the answer is correct
upvoted 23 times

ozbonny Most Recent 6 months, 4 weeks ago
Selected Answer: B
Correct is B
upvoted 1 times

vsvaid 9 months ago
Selected Answer: B
Continued Assurance
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: B
Definitely no is the answer
upvoted 1 times

Govcomm 2 years, 1 month ago
Continuous Assurance
upvoted 1 times

Cheehp 2 years, 5 months ago
Selected during exam.
No.
upvoted 1 times

rdemontis 2 years, 6 months ago
Selected Answer: B
correct answer. CI doesn't limit project configuration
upvoted 1 times

idrisfl 2 years, 8 months ago
I guess this question is no longer relevant, the link suggests AzSk was retired in FY21
upvoted 1 times

V_Ramon 3 years, 1 month ago

this question came out today, July 28, 2021

upvoted 4 times

Abhi26 3 years, 8 months ago

Correct Ans :yes

upvoted 1 times

nasa1515 3 years, 8 months ago

answer is no

upvoted 18 times

Question #22 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You manage a project in Azure DevOps.
You need to prevent the configuration of the project from changing over time.
Solution: Implement Continuous Assurance for the project.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
The basic idea behind Continuous Assurance (CA) is to setup the ability to check for "drift" from what is considered a secure snapshot of a system. Support for
Continuous Assurance lets us treat security truly as a 'state' as opposed to a 'point in time' achievement. This is particularly important in today's context when
'continuous change' has become a norm.
There can be two types of drift:
➪ Drift involving 'baseline' configuration: This involves settings that have a fixed number of possible states (often pre-defined/statically determined ones). For instance, a SQL DB can have TDE encryption turned ON or OFFา€¦or a Storage Account may have auditing turned ON however the log retention period may be less than 365 days.
➪ Drift involving 'stateful' configuration: There are settings which cannot be constrained within a finite set of well-known states. For instance, the IP addresses configured to have access to a SQL DB can be any (arbitrary) set of IP addresses. In such scenarios, usually human judgment is initially required to determine whether a particular configuration should be considered 'secure' or not. However, once that is done, it is important to ensure that there is no "stateful drift" from the attested configuration. (E.g., if, in a troubleshooting session, someone adds the IP address of a developer machine to the list, the Continuous Assurance feature should be able to identify the drift and generate notifications/alerts or even trigger 'auto-remediation' depending on the severity of the change).
Reference:
https://azsk.azurewebsites.net/04-Continous-Assurance/Readme.html

Community vote distribution

A (100%)

ChauPhan Highly Voted 2 years, 10 months ago
IMPORTANT: DevOps Kit (AzSK) is being sunset by end of FY21
upvoted 6 times

jay158 2 years, 4 months ago
https://github.com/azsk/AzTS-docs
is replacement of DevOps Kit (AzSK)
upvoted 1 times

vsvaid Most Recent 9 months ago
Selected Answer: A
Agree to suggested answer
upvoted 1 times

col2511kol 1 year, 5 months ago
Selected Answer: A
you can combine Continuous Assurance with access controls to help prevent the configuration of an Azure DevOps project from changing over time. By using access controls and other security best practices, you can limit the ability of users to make unauthorized changes to the project configuration. Continuous Assurance, on the other hand, will monitor for any drift from the desired or secure state and alert you if any changes occur.
upvoted 3 times

adityagoel26 1 year, 6 months ago

According to chatGPT,

B. No.

Continuous Assurance is a real feature, but it is not related to preventing configuration changes over time. Instead, it is a security feature that continuously monitors your Azure DevOps organization for vulnerabilities, configuration issues, and potential security threats. To prevent configuration changes over time, you may consider implementing some of the following:

Implement a code review process for any changes made to the project configuration.
Use version control to manage changes to the project configuration.
Implement policies in Azure DevOps that prevent changes to critical configuration settings.
Use Azure DevOps audit logs to monitor changes to the project configuration.

upvoted 2 times

syu31svc 2 years, 1 month ago

Selected Answer: A

https://www.microsoft.com/en-us/insidetrack/building-cloud-apps-using-the-secure-devops-kit-for-azure:

"Continuous assurance prevents security state drift, helps to stay current with Azure security feature improvements"

Answer is Yes

upvoted 2 times

Govcomm 2 years, 1 month ago

Correct, continuous assurance

upvoted 1 times

prashantjoge 2 years, 5 months ago

The closest answer to this is azure app configuration. App configuration supports
- Microservices based on Azure Kubernetes Service, Azure Service Fabric, or other containerized apps deployed in one or more geographies
- Serverless apps, which include Azure Functions or other event-driven stateless compute apps
- Continuous deployment pipeline

upvoted 1 times

prashantjoge 2 years, 5 months ago

Dont think this question is relevant anaymore

upvoted 3 times

rdemontis 2 years, 6 months ago

Selected Answer: A

correct explanation

upvoted 1 times

goatlord 3 years, 1 month ago

Biggest Correct Here.

upvoted 4 times

Johnnien 3 years, 9 months ago

CA correct

upvoted 4 times

Question #23 *Topic 3*

You are designing a configuration management solution to support five apps hosted on Azure App Service. Each app is available in the following three environments: development, test, and production.

You need to recommend a configuration management solution that meets the following requirements:

- Supports feature flags
- Tracks configuration changes from the past 30 days
- Stores hierarchically structured configuration values
- Controls access to the configurations by using role-based access control (RBAC) permissions
- Stores shared values as key/value pairs that can be used by all the apps

Which Azure service should you recommend as the configuration management solution?

A. Azure Cosmos DB

B. Azure App Service

C. Azure App Configuration

D. Azure Key Vault

Suggested Answer: *C*

The Feature Manager in the Azure portal for App Configuration provides a UI for creating and managing the feature flags that you use in your applications.

App Configuration offers the following benefits:

- A fully managed service that can be set up in minutes
- Flexible key representations and mappings
- Tagging with labels
- Point-in-time replay of settings
- Dedicated UI for feature flag management
- Comparison of two sets of configurations on custom-defined dimensions

Enhanced security through Azure-managed identities

-
- Encryption of sensitive information at rest and in transit
- Native integration with popular frameworks

App Configuration complements Azure Key Vault, which is used to store application secrets.

Reference:

https://docs.microsoft.com/en-us/azure/azure-app-configuration/overview

Community vote distribution

C (100%)

ankit38g Highly Voted 3 years, 2 months ago

Given answer is correct.

C, Azure App Configuration

upvoted 17 times

Optimist_Indian Highly Voted 2 years, 7 months ago

Got this question in Feb-2022 exam (scored 910+). Given answer is correct : C.

upvoted 12 times

ozbonny Most Recent 6 months, 4 weeks ago

Selected Answer: C

Correct C

upvoted 1 times

vsvaid 9 months ago

Selected Answer: C

Agree with suggested answer

upvoted 1 times

yana_b 1 year, 1 month ago

Selected Answer: C

correct

upvoted 1 times

renzoku 1 year, 2 months ago

Selected Answer: C

C. Azure App Configuration.

Support for feature flags.

Allowing you to track and review changes.

Supports hierarchical key-value configurations.

Allowing you to implement RBAC.

Provides a centralized configuration store that can be used by multiple apps.

Azure Key Vault

Share values as secret but may not offer a good level of flexibility.

NOT: feature flags, tracking configuration changes, organizing configuration values hierarchically, support RBAC for managing secrets.

Azure Cosmos DB

Offer built-in RBAC mechanisms, Focused on data storage rather sharing values across multiples apllications.

NOT: feature flags, tracking configuration changes, organizing configuration values hierarchically.

Azure App Service

Supports storing shared configuration values that can be accessed by multiple applications.

NOT: feature flags, tracking configuration changes, organizing configuration values hierarchically, granular RBAC permissions.

upvoted 3 times

zellck 1 year, 3 months ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/azure-app-configuration/overview

Azure App Configuration provides a service to centrally manage application settings and feature flags. Modern programs, especially programs running in a cloud, generally have many components that are distributed in nature. Spreading configuration settings across these components can lead to hard-to-troubleshoot errors during an application deployment. Use App Configuration to store all the settings for your application and secure their accesses in one place.

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: C

From https://docs.microsoft.com/en-us/azure/azure-app-configuration/overview:

"Azure App Configuration provides a service to centrally manage application settings and feature flags"

C is the answer

upvoted 1 times

Govcomm 2 years, 1 month ago

Azure App Service App Configuration.

upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: C

correct answer

upvoted 1 times

Question #24 *Topic 3*

You have a containerized solution that runs in Azure Container Instances. The solution contains a frontend container named App1 and a backend container named DB1. DB1 loads a large amount of data during startup.
You need to verify that DB1 can handle incoming requests before users can submit requests to App1.
What should you configure?

A. a liveness probe

B. a performance log

C. a readiness probe

D. an Azure Load Balancer health probe

Suggested Answer: *C*
For containerized applications that serve traffic, you might want to verify that your container is ready to handle incoming requests. Azure Container Instances supports readiness probes to include configurations so that your container can't be accessed under certain conditions.
Incorrect Answers:
A: Containerized applications may run for extended periods of time, resulting in broken states that may need to be repaired by restarting the container. Azure
Container Instances supports liveness probes so that you can configure your containers within your container group to restart if critical functionality is not working.
Reference:
https://docs.microsoft.com/en-us/azure/container-instances/container-instances-readiness-probe

Community vote distribution

C (100%)

kumardeb Highly Voted 3 years, 10 months ago
C. a readiness probe
upvoted 17 times

basw77 Highly Voted 2 years, 2 months ago
Selected Answer: C
To check if READY, use READIness probe
upvoted 12 times

vsvaid Most Recent 9 months ago
Selected Answer: C
Readiness probe
upvoted 1 times

flafernan 1 year ago
Selected Answer: C
Within a container instance, to check whether a DB is already able to receive requests and receive traffic, you need to configure the:
Ready probe.
Just to illustrate, the Liveness probe only checks whether the resource inside the container is active (and can restart if it is not satisfied), and cannot necessarily receive requests. These are the differences between the two features. Talking about receiving requests is the Readiness probe.
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: C
readiness probe, as it verifies whether traffic request could be handled
upvoted 1 times

renzoku 1 year, 2 months ago
Selected Answer: C
C. a readiness probe
Check if a container is ready to handle incoming requests.

Liveness probe, used to determinate if a container is still running adn functioning properly.
upvoted 1 times

zellck 1 year, 3 months ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/container-instances/container-instances-readiness-probe
For containerized applications that serve traffic, you might want to verify that your container is ready to handle incoming requests. Azure Container Instances supports readiness probes to include configurations so that your container can't be accessed under certain conditions. The readiness probe behaves like a Kubernetes readiness probe. For example, a container application might need to load a large data set during startup, and you don't want it to receive requests during this time.
upvoted 2 times

syu31svc 2 years, 1 month ago

Selected Answer: C

C pretty much gives it away as the answer don't you think?
upvoted 2 times

Govcomm 2 years, 1 month ago

readiness probe ensure the system is ready to accept request
liveness probe is used to determine whether the system is responsive or not. And reboot the system when the system becomes unresponsive.
upvoted 4 times

UnknowMan 2 years, 4 months ago

Correct, with a readness prob we can make the app "offline" (off for the load balancer) , on remake it online when the condition is ok
upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: C

correct answer and documentation provided
upvoted 3 times

joydinesh07 2 years, 8 months ago

C. a readiness probe
upvoted 1 times

RajatSahani 2 years, 9 months ago

readiness probe
upvoted 1 times

chahine 2 years, 11 months ago

Agree : Kubernetes uses readiness probes to decide when the container is available for accepting traffic. The readiness probe is used to control which pods are used as the backends for a service
upvoted 1 times

goatlord 3 years, 1 month ago

I have readiness to call this one CORRECT
upvoted 2 times

peter201013 3 years, 6 months ago

Agree with the answer
upvoted 2 times

Question #25 *Topic 3*

You are designing a strategy to monitor the baseline metrics of Azure virtual machines that run Windows Server.
You need to collect detailed data about the processes running in the guest operating system.
Which two agents should you deploy? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. the Telegraf agent

B. the Azure Log Analytics agent

C. the Azure Network Watcher Agent for Windows

D. the Dependency agent

Suggested Answer: *BD*
The following table provide a quick comparison of the Azure Monitor agents for Windows.

	Azure Monitor agent (preview)	**Diagnostics extension (WAD)**	**Log Analytics agent**	**Dependency agent**
Environments supported	Azure	Azure	Azure Other cloud On-premises	Azure Other cloud On-premises
Agent requirements	None	None	None	Requires Log Analytics agent
Data collected	Event Logs Performance	Event Logs ETW events Performance File based logs IIS logs .NET app logs Crash dumps Agent diagnostics logs	Event Logs Performance File based logs IIS logs Insights and solutions Other services	Process dependencies Network connection metrics
Data sent to	Azure Monitor Logs Azure Monitor Metrics	Azure Storage Azure Monitor Metrics Event Hub	Azure Monitor Logs	Azure Monitor Logs (through Log Analytics agent)

Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview

Community vote distribution
BD (100%)

Dalias Highly Voted 3 years, 2 months ago
got this in 30 Jun 2021 exams. scored 800+ marks. answer is right
upvoted 15 times

Inno250 Highly Voted 3 years, 4 months ago
correct
upvoted 7 times

arr73 Most Recent 4 months, 3 weeks ago

Selected Answer: BD

Answer BD is correct but an updated version should consider "Azure Monitor Agent" instead of "Azure Log Analytics agent", because documentation says that "The Log Analytics agent is on a deprecation path and won't be supported after August 31, 2024. Any new data centers brought online after January 1 2024 will not support the Log Analytics agent. If you use the Log Analytics agent to ingest data to Azure Monitor, migrate to the new Azure Monitor agent prior to that date."
Reference:
https://learn.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent

upvoted 2 times

ozbonny 6 months, 4 weeks ago

Selected Answer: BD

Correct B and D

upvoted 1 times

yana_b 1 year, 1 month ago

Selected Answer: BD

clearly evidenced by the provided print screen

upvoted 1 times

zellck 1 year, 3 months ago

Selected Answer: BD

BD is the answer.

https://learn.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent#primary-scenarios
Use the Log Analytics agent if you need to:
- Collect logs and performance data from Azure virtual machines or hybrid machines hosted outside of Azure.
- Use VM insights, which allows you to monitor your machines at scale and monitor their processes and dependencies on other resources and external processes.

https://learn.microsoft.com/en-us/azure/azure-monitor/vm/vminsights-dependency-agent-maintenance
The Dependency Agent collects data about processes running on the virtual machine and external process dependencies.

upvoted 2 times

Jawad1462 1 year, 10 months ago

Selected Answer: BD

Correct

upvoted 1 times

Yatoom 1 year, 10 months ago

The Log Analytics Agent is now replaced by the Azure Monitor Agent. See https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview.

upvoted 4 times

syu31svc 2 years, 1 month ago

Selected Answer: BD

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview:

Log Analytics agent is one of the agents for Windows

"On hybrid machines, use Azure Arc-enabled servers to deploy the Azure Monitor agent, Log Analytics, and Azure Monitor Dependency VM extensions"

B and D

upvoted 1 times

Govcomm 2 years, 1 month ago

Dependency agent: processes running in the system
Azure Log Analytic agent: collect the information and send to the Azure Monitor.

upvoted 2 times

rdemontis 2 years, 6 months ago

Selected Answer: BD

Correct answers as the documentation provided demonstrate

upvoted 3 times

goatlord 3 years, 1 month ago

Dependency Agent? Isn't it Network Watcher?

upvoted 2 times

BasAZ 2 years, 9 months ago

Network watcher is a VM-extension and not an agent u can deploy

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview

So I think A + D is correct

upvoted 2 times

BasAZ 2 years, 9 months ago

B + D ****

Given answer correct

upvoted 1 times

DRAG DROP -

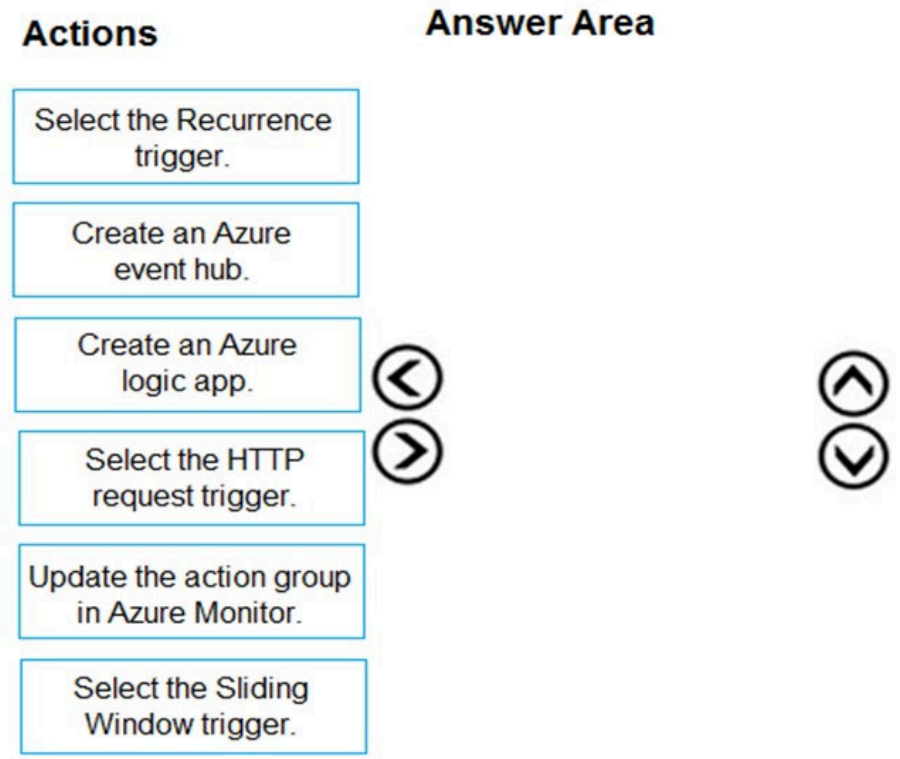
You use Azure Pipelines to automate Continuous Integration/Continuous Deployment (CI/CD) for an Azure web app named WebApp1.

You configure an Azure Monitor alert that is triggered when WebApp1 generates an error.

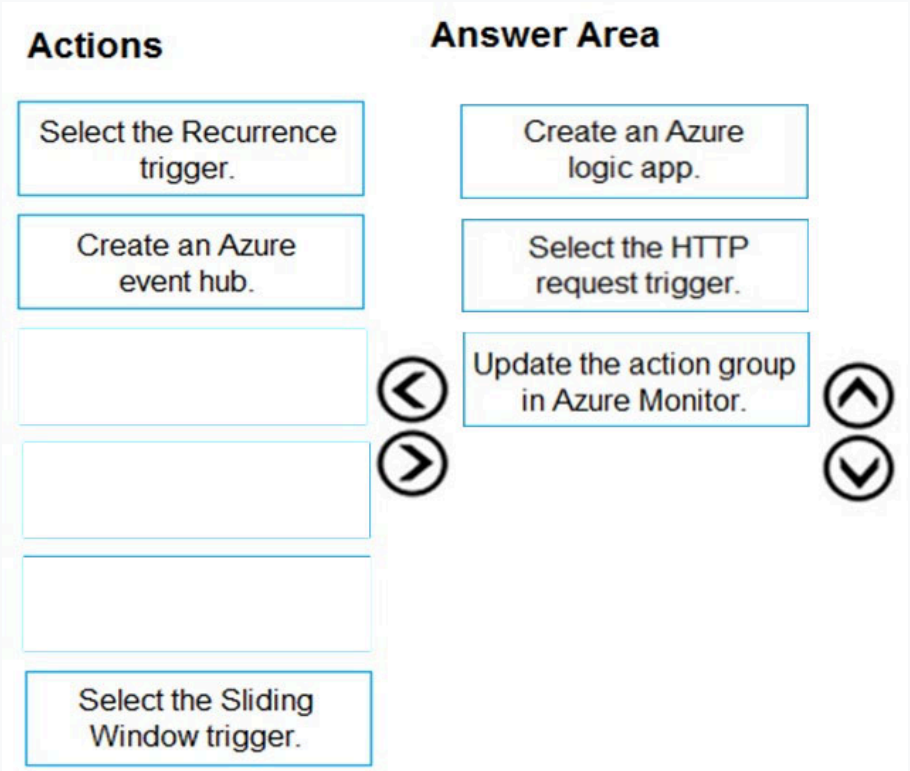
You need to configure the alert to forward details of the error to a third-party system. The solution must minimize administrative effort.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Suggested Answer:



Box 1: Create an Azure logic app.

Box 2: Select the HTTP request trigger.

Box 3: Updated the action group in Azure Monitor.

Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups-logic-app

renzoku Highly Voted 1 year, 2 months ago
WebApp1 generates an error > trigger an alert (Azure Monitor) > forward details of the error (Azure logic app) > Third-party system

1. Create an Azure logic app
This will serve for processing and forwarding the error.

2. Select the HTTP request trigger
In Logic app, configure a HTTP trigger, this will receive the error details from the alert.

3. Update the action group in Azure Monitor
Update the action group in Azure Monitor associated with the alert.
Add a new action to the action group, this will ensure that when the alert is triggered due to an error in WebApp1, the error details are sent to the Logic App via an HTTP request.

Azure Event Hub may not be the best fit for forwarding details of the error to a third-party system. It is typically used for ingesting and processing large volumes of data from various sources.
upvoted 18 times

Joe_Mauma 1 year, 1 month ago
Thank you
upvoted 1 times

zellck Highly Voted 1 year, 3 months ago
1. Create Azure logic app
2. Select HTTP request trigger
3. Update action group in Azure Monitor

https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-logic-apps?tabs=send-email#create-a-logic-app
upvoted 9 times

vsvaid Most Recent 9 months ago
box 2,3 and 4
upvoted 1 times

yana_b 1 year, 1 month ago
Provided answer seems to be correcr:
1.Create AZ logic app
2. Select HTTP request trigger
3. Update the AZ group in AZ Monitor
upvoted 1 times

fkaracan 1 year, 7 months ago
correct
upvoted 1 times

pat1892 1 year, 10 months ago
Should be correct!
upvoted 6 times

syu31svc 2 years, 1 month ago
https://docs.microsoft.com/en-us/azure/connectors/connectors-native-recurrence

recurrence and sliding window triggers are not part of the answers

logic app over event hub

Answer is correct
upvoted 2 times

hebertpena88 2 years, 1 month ago

Loks correct for me :)

upvoted 1 times

Govcomm 2 years, 1 month ago

Logic App

Request trigger

Azure Monitor action group

upvoted 3 times

resonant 1 year ago

I also think it should be the Request trigger instead of HTTP, but that option is not available

upvoted 1 times

UnknowMan 2 years, 4 months ago

correct

upvoted 2 times

U3 2 years, 4 months ago

I think Correct!

upvoted 1 times

Question #27 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure DevOps organization named Contoso and an Azure subscription. The subscription contains an Azure virtual machine scale set named VMSS1 that is configured for autoscaling.
You have a project in Azure DevOps named Project1. Project1 is used to build a web app named App1 and deploy App1 to VMSS1.
You need to ensure that an email alert is generated whenever VMSS1 scales in or out.
Solution: From Azure DevOps, configure the Notifications settings for Project1.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Notifications help you and your team stay informed about activity that occurs within your projects in Azure DevOps. You can get notified when changes occur to the following items:
➪ work items
➪ code reviews
➪ pull requests
➪ source control files
builds
▪
Reference:
https://docs.microsoft.com/en-us/azure/devops/notifications/about-notifications?view=azure-devops

Community vote distribution
B (100%)

syu31svc Highly Voted 2 years, 1 month ago
Selected Answer: B
Answer is No

Configure settings in VMSS and not the project

https://docs.microsoft.com/en-us/azure/azure-monitor/autoscale/autoscale-webhook-email
upvoted 8 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: B
VMs notifications would be on azure monitor or Azure Autoscale
upvoted 1 times

vsvaid 9 months ago
Selected Answer: B
Use notification setting in scale set
upvoted 2 times

yana_b 1 year, 1 month ago
Selected Answer: B
correct answer is no
upvoted 1 times

Omarook 1 year, 5 months ago
Selected Answer: B
Correct is B

upvoted 1 times

Govcomm 2 years, 1 month ago

Azure Monitor action group for the autoscale of VMSS

upvoted 3 times

Juancho2507 2 years, 2 months ago

Selected Answer: B

Yes, it is correct, https://docs.microsoft.com/en-us/azure/devops/notifications/about-notifications?view=azure-devops

upvoted 1 times

sghaha 2 years, 3 months ago

is B correct?

upvoted 1 times

Divyayuvi 2 years, 2 months ago

yes, its correct.

upvoted 1 times

Juancho2507 2 years, 2 months ago

Yes, cause you have to configure the notifications setting in the VMSS1 not in the project1

upvoted 2 times

Question #28 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure DevOps organization named Contoso and an Azure subscription. The subscription contains an Azure virtual machine scale set named VMSS1 that is configured for autoscaling.
You have a project in Azure DevOps named Project1. Project1 is used to build a web app named App1 and deploy App1 to VMSS1.
You need to ensure that an email alert is generated whenever VMSS1 scales in or out.
Solution: From Azure DevOps, configure the Service hooks settings for Project1.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Community vote distribution

B (100%)

ozbonny 6 months, 3 weeks ago

Selected Answer: B

VMs notifications would be on azure monitor or Azure Autoscale

upvoted 1 times

vsvaid 9 months ago

Selected Answer: B

Use notification set in scale set

upvoted 1 times

yana_b 1 year, 1 month ago

Selected Answer: B

correct

upvoted 1 times

Omarook 1 year, 5 months ago

Selected Answer: B

Correct

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: B

This is 100% No

upvoted 4 times

Govcomm 2 years, 1 month ago

Azure Monitor action group for the autoscale of VMSS

upvoted 1 times

Dileep75 2 years, 2 months ago

service hooks required to integrate with azure devops. enabling notification in vmss is correct

upvoted 2 times

Eltooth 2 years, 3 months ago

Selected Answer: B

B is correct answer. Should be Azure Monitor.

upvoted 3 times

Question #29 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure DevOps organization named Contoso and an Azure subscription. The subscription contains an Azure virtual machine scale set named VMSS1 that is configured for autoscaling.
You have a project in Azure DevOps named Project1. Project1 is used to build a web app named App1 and deploy App1 to VMSS1.
You need to ensure that an email alert is generated whenever VMSS1 scales in or out.
Solution: From Azure Monitor, create an action group.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
An action group is a collection of notification preferences defined by the owner of an Azure subscription. Azure Monitor, Service Health and Azure Advisor alerts use action groups to notify users that an alert has been triggered.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups

Community vote distribution
A (100%)

Fastdruid Highly Voted 1 year, 5 months ago
I don't believe this is correct, an action group defines actions including emailing but NOT which alerts they would respond to. By itself just setting up an action group does NOT meet the goal.

You need to setup an alert rule to define the condition (in this case scaling in or out) which would then perform the actions defined in the action group. Without the alert rule the action group does nothing. It would certainly be part of the solution but doesn't by itself meet the goal.
upvoted 6 times

xRiot007 1 year, 2 months ago
Maybe that part is already implemented. How do you understand this ? "When Azure Monitor data indicates that there might be a problem with your infrastructure or application, an alert is triggered. " If this already done and the alert is triggered then I think we just need to setup the action group
upvoted 1 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: A
Correct A
upvoted 1 times

vsvaid 9 months ago
Selected Answer: A
Agree with suggested answer
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: A
correct
upvoted 1 times

zellck 1 year, 3 months ago
Selected Answer: A
A is the answer.

https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups
When Azure Monitor data indicates that there might be a problem with your infrastructure or application, an alert is triggered. Alerts can contain action groups, which are a collection of notification preferences. Azure Monitor, Azure Service Health, and Azure Advisor use action groups to notify users about the alert and take an action.

Each action is made up of the following properties:
- Type: The notification that's sent or action that's performed. Examples include sending a voice call, SMS, or email. You can also trigger various types of automated actions.
- Name: A unique identifier within the action group.
- Details: The corresponding details that vary by type.
upvoted 2 times

hung1995 1 year, 4 months ago
A is correct answer.
upvoted 1 times

Narender_892 2 years ago
Yes, creating an action group is the correct answer.
upvoted 4 times

syu31svc 2 years, 1 month ago
Selected Answer: A
Yes definitely

This is what we need
upvoted 1 times

kennynelcon 2 years, 1 month ago
Selected Answer: A
Seen this previously and it is accurate.
upvoted 1 times

Govcomm 2 years, 1 month ago
Azure Monitor action group for the autoscale of VMSS
upvoted 2 times

Eltooth 2 years, 3 months ago
Selected Answer: A
A is correct answer.
Azure Monitor is used to monitor resource metrics (VMSS scale out) with action group to email/sms/trigger function app for notification.
upvoted 3 times

swaycloud 2 years, 3 months ago
Correct
upvoted 2 times

Question #30 *Topic 3*

DRAG DROP -

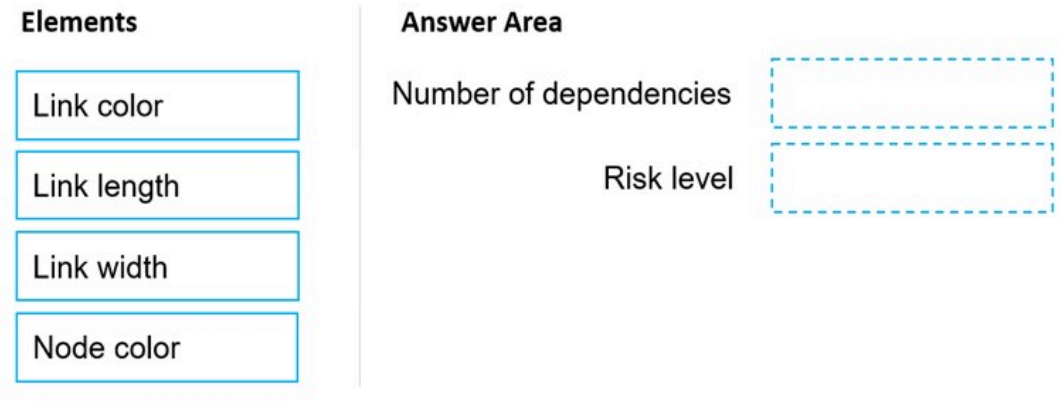
You are using the Dependency Tracker extension in a project in Azure DevOps.

You generate a risk graph for the project.

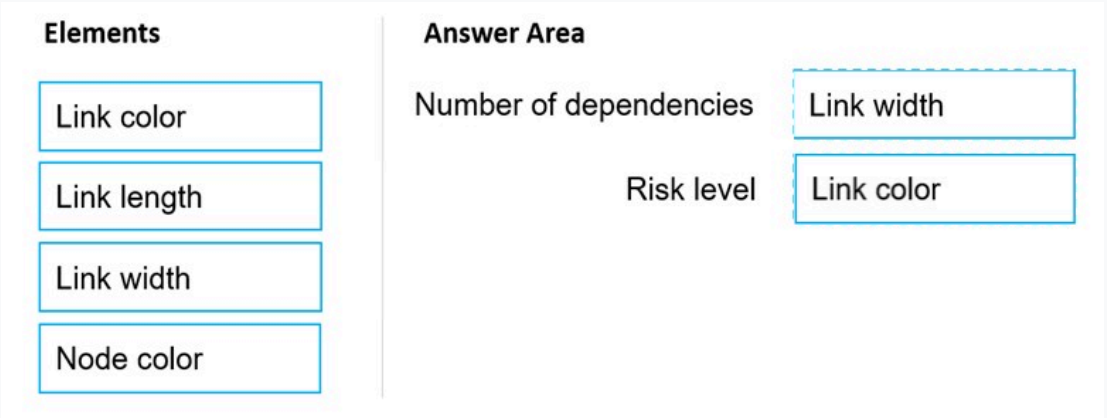
What should you use in the risk graph to identify the number of dependencies and the risk level of the project? To answer, drag the appropriate elements to the correct data points. Each element may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested Answer:



Box 1: Link width -

The width of the lines indicates how many dependencies exist in that area, the thicker the link the more dependencies as indicated in the legend.

Box 2: Link color -

Reference:

https://docs.microsoft.com/en-us/azure/devops/boards/extensions/dependency-tracker?view=azure-devops#risk-graph

zellck Highly Voted 1 year, 3 months ago

1. Link width
2. Link color

https://learn.microsoft.com/en-us/azure/devops/extensions/dependency-tracker/risk-graph

The color coding in the risk graph is dependent on the State of the item and is configurable. The width of the lines in the risk graph indicate how many dependencies exist in that area, the thicker the link the more dependencies.

upvoted 16 times

yana_b Most Recent 1 year, 1 month ago

1. Link width
2. Link color

refer to the link provided by zellck

upvoted 3 times

RonZhong 1 year, 5 months ago

Link Color:

- Red: At Risk or Not On Track
- Green: On Track

Link Width: The width of the lines indicates how many dependencies exist in that area, the thicker the link the more dependencies as indicated in the legend.

upvoted 3 times

fkaracan 1 year, 7 months ago

I think it's Node color.

Node color is used to represent the state or characteristics of an individual node in a graph. For example, in a risk graph, node color could be used to indicate the level of risk associated with a particular component of an application. For example, components with a high risk score could be displayed in red, while components with a low risk score could be displayed in green.

Link color is used to represent the relationship or connection between two nodes in a graph. For example, in a risk graph, link color could be used to indicate the strength of the dependency between two components. A strong link between two components could be displayed in one color, while a weak link could be displayed in another color.

upvoted 1 times

fkaracan 1 year, 7 months ago

ignore my comment it's link color.

upvoted 4 times

markp 2 years ago

I think this question is no more relevant because the Dependency Tracker extension is not supported by any product group. Microsoft recommends to use Delivery Plans to track dependencies instead of Dependency Tracker:
https://docs.microsoft.com/en-us/azure/devops/boards/extensions/dependency-tracker?view=azure-devops

upvoted 4 times

pdk88 1 year, 11 months ago

This is a pretty new question, so it's definitly relevant ;)

upvoted 5 times

syu31svc 2 years ago

Answer is correct and provided link supports it

upvoted 3 times

HOTSPOT -

You have an Azure subscription that contains the resources shown in the following table.

Name	Type
DF1	Azure Data Factory
SQL1	Azure SQL Database
KV1	Azure Key Vault

You plan to create a linked service in DF1. The linked service will connect to SQL1 by using Microsoft SQL Server authentication. The password for the SQL

Server login will be stored -

in KV1.

You need to configure DF1 to retrieve the password when the data factory connects to SQL1. The solution must use the principle of least privilege.

How should you configure DF1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

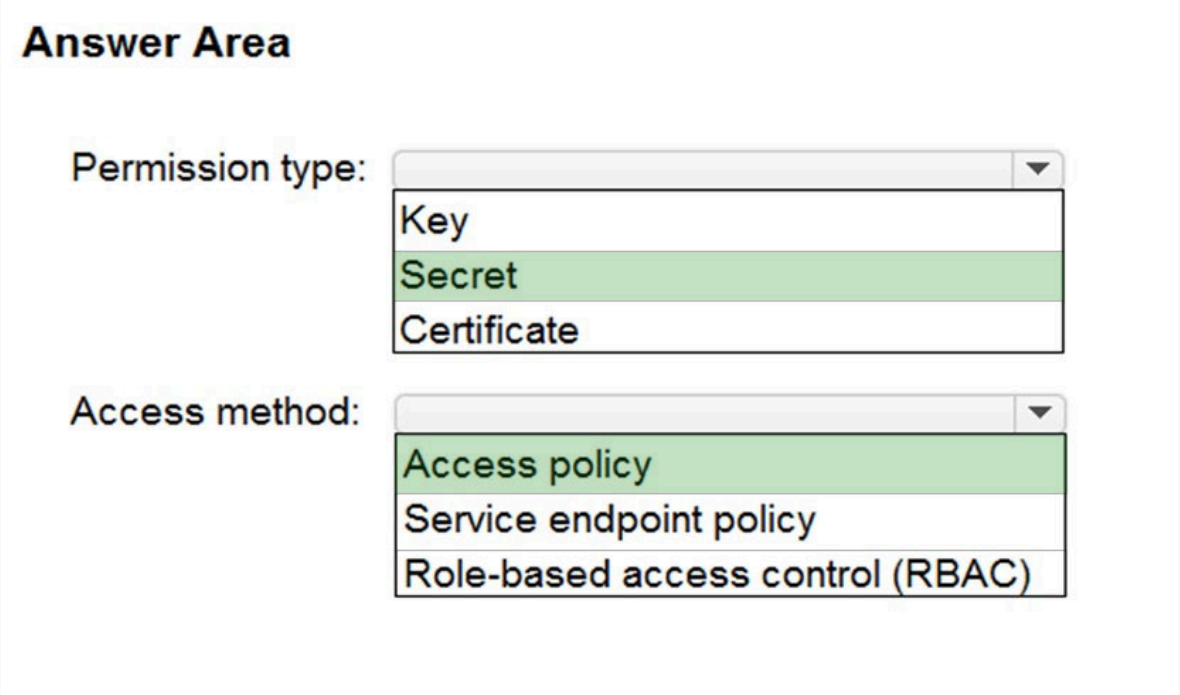
Permission type:

- Key
- Secret
- Certificate

Access method:

- Access policy
- Service endpoint policy
- Role-based access control (RBAC)

Suggested Answer:



Box 1: Secret -
Store credential in Azure Key Vault by reference secret stored in key vault.
To reference a credential stored in Azure Key Vault, you need to:
1. Retrieve data factory managed identity
2. Grant the managed identity access to your Azure Key Vault. In your key vault -> Access policies -> Add Access Policy, search this managed identity to grant
Get permission in Secret permissions dropdown. It allows this designated factory to access secret in key vault.
3. Create a linked service pointing to your Azure Key Vault.
4. Create data store linked service, inside which reference the corresponding secret stored in key vault.

Box 2: Access policy -
Reference:
https://docs.microsoft.com/en-us/azure/data-factory/store-credentials-in-key-vault

surensaluka Highly Voted 1 year, 7 months ago
This came today (2023-02-14) for my exam. Selected Secret and Access Policy
upvoted 14 times

pc1707 1 year, 1 month ago
Hey! Did you get simulation questions?
upvoted 5 times

meoukg Highly Voted 1 year, 10 months ago
saw it yesterday in my exam
upvoted 9 times

pc1707 1 year, 1 month ago
Hey! Did you get simulation questions?
upvoted 2 times

Skankhunt Most Recent 1 month, 3 weeks ago
It's an old question. I believe the correct answer now would be:
Secret
RBAC
upvoted 4 times

ozbonny 6 months, 3 weeks ago
secret
access policy
upvoted 1 times

vsvaid 9 months ago
Agree with suggested answer
upvoted 1 times

Rod_DA 11 months, 4 weeks ago
New recommended acceess configuration to vault is now RBAC instead of access policy and there is a role to give access only to secrets so The answer should be secret and RBAC
upvoted 6 times

Tyler2023 1 year ago
Access Policy is a legacy authorization system built in Key Vault to provide access to keys, secrets, and certificates but there is new recommended authorization, which is RBAC, you can setup the Managed Identity of Azure Data Factory and allow the identity to access Key Vault BUT since, in the question, they ask which permission type that you need which is Secret so you have to Access Policy instead of RBACK

Answer is Secret and Access Policy

refs:
https://learn.microsoft.com/en-us/azure/data-factory/data-factory-service-identity
https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-access-policy
upvoted 5 times

yana_b 1 year, 1 month ago
Provided answer is correct
upvoted 1 times

xRiot007 1 year, 2 months ago
Answer is secret and access policy. See ref: https://tech-tutes.com/2020/05/16/get-database-password-from-key-vault-in-data-factory/
upvoted 1 times

zellck 1 year, 3 months ago
1. Secret
2. Access policy

https://learn.microsoft.com/en-us/azure/key-vault/general/assign-access-policy?tabs=azure-portal
A Key Vault access policy determines whether a given security principal, namely a user, application or user group, can perform different operations on Key Vault secrets, keys, and certificates. You can assign access policies using the Azure portal, the Azure CLI, or Azure PowerShell.
upvoted 6 times

dibbadobbagibbu 1 year, 6 months ago
RBAC is the only one than can limit access per Secret. So you could argue that Rbac is correct
upvoted 1 times

Rubends 1 year, 5 months ago
RBAC is use for keyvault access for use secret you must configure access policy
upvoted 1 times

catfood 1 year, 2 months ago
no, rbac can be used for individual secrets, configure in the secret's IAM blade.
upvoted 2 times

Pav143 3 months ago
Well, now that means RBAC for individual secret access satisfies for least privilege than an access policy that offers high privilege by giving access to ALL secrets. So yeah, microsoft is not dumb, if you select access policy when there is RBAC in the options, youre going to lose a point there for sure.
upvoted 1 times

Aqlanoz 1 year, 6 months ago
since keyvault have rbac now, should the answer be rbac instead of access policy ?
upvoted 5 times

syu31svc 2 years, 1 month ago
"Password" so secret for permission

Access to Key Vault so Access Policy

Answer is correct

upvoted 3 times

Govcomm 2 years, 1 month ago

Secret

Access Policy (Data Plan)

upvoted 4 times

Leandrocei 2 years, 2 months ago

Correct. Came today 22 july 9

upvoted 4 times

UnknowMan 2 years, 4 months ago

Secret (Password is stored) And Access Policy

upvoted 3 times

ppo12 2 years, 4 months ago

I think correct, since password usually stored in Secret,

No need to give RBAC, access policy will do

upvoted 4 times

Question #2 *Topic 4*

You have several Azure Active Directory (Azure AD) accounts.
You need to ensure that users use multi-factor authentication (MFA) to access Azure apps from untrusted networks.
What should you configure in Azure AD?

A. access reviews

B. managed identities

C. entitlement management

D. conditional access

Suggested Answer: *D*
You can configure a Conditional Access policy that requires MFA for access from untrusted networks.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa

Community vote distribution

D (100%)

ozbonny 6 months, 3 weeks ago

Selected Answer: D

Correct D
I found this also: https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview

upvoted 1 times

vsvaid 9 months ago

Selected Answer: D

Agree to

upvoted 1 times

yana_b 1 year, 1 month ago

Selected Answer: D

Conditional access

upvoted 1 times

renzoku 1 year, 2 months ago

Selected Answer: D

D. conditional access
You can enforce policies that control access to your Azure Apps, e.g. require MFA to users

upvoted 1 times

Omarook 1 year, 5 months ago

Selected Answer: D

Correct

upvoted 1 times

ABC666 1 year, 8 months ago

Selected Answer: D

Conditional access.

upvoted 2 times

Matharax 1 year, 11 months ago

Selected Answer: D

Conditional access allows you to add 'policies' to Azure active directory.

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: D

You have to ensure MFA so answer is D for sure

upvoted 1 times

Govcomm 2 years, 1 month ago

Azure AD Conditional Access

upvoted 1 times

kennynelcon 2 years, 2 months ago

Selected Answer: D

AZ - 104

upvoted 4 times

deltarj 2 years, 3 months ago

Selected Answer: D

correct

upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 1 times

U3 2 years, 4 months ago

Correct Answer!

upvoted 1 times

Question #3 *Topic 4*

You plan to provision a self-hosted Linux agent.
Which authentication mechanism should you use to register the self-hosted agent?

A. personal access token (PAT)

B. SSH key

C. Alternate credentials

D. certificate

Suggested Answer: *A*
Note: PAT Supported only on Azure Pipelines and TFS 2017 and newer. After you choose PAT, paste the PAT token you created into the command prompt window. Use a personal access token (PAT) if your Azure DevOps Server or TFS instance and the agent machine are not in a trusted domain. PAT authentication is handled by your Azure DevOps Server or TFS instance instead of the domain controller.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/v2-linux

Community vote distribution

A (100%)

kumardeb Highly Voted 3 years, 10 months ago
A. personal access token (PAT)
upvoted 21 times

Hooters Highly Voted 3 years, 10 months ago
Should be A. personal access token (PAT)
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/v2-linux?view=azure-devops
upvoted 11 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: A
Correct A
during the learning path it recommended to use PAT
upvoted 2 times

saket051985 7 months, 2 weeks ago
When provisioning a self-hosted Linux agent in Azure DevOps, you should use an SSH key for authentication to register the agent. Azure DevOps uses the SSH protocol for secure communication with the self-hosted agent.
upvoted 1 times

vsvaid 9 months ago
Selected Answer: A
Personal Access Token
upvoted 1 times

Omarook 1 year, 5 months ago
Selected Answer: A
Correct
upvoted 2 times

Fal991l 1 year, 5 months ago
GPT: PATs are typically used to authenticate users or services to Azure DevOps resources, and are not specifically designed for registering self-hosted agents. Additionally, using a PAT for authentication would require the PAT to be stored on the machine hosting the self-hosted agent, which could potentially pose a security risk if the machine were compromised.

A more secure and recommended authentication mechanism for registering a self-hosted Linux agent would be to use an SSH key. SSH keys are a common and secure way to authenticate to remote machines using public-key cryptography, and are widely supported in the Linux ecosystem. They also do not require the sharing or storage of any sensitive information like a PAT.

Therefore, if given the choice, I would recommend using an SSH key as the authentication mechanism for registering a self-hosted Linux agent over a personal access token.
upvoted 1 times

Fal991l 1 year, 5 months ago
GPT:If only one option is allowed and the question specifically asks for the authentication mechanism to register a self-hosted Linux agent, and based on the available options, I would agree that choosing "personal access token (PAT)" is likely the best choice in the context of the AZ-400 exam.

While using an SSH key is more secure, it's possible that the exam question may have constraints or requirements that make using an SSH key not feasible or desirable. Additionally, the use of a personal access token (PAT) is a common authentication mechanism in Azure DevOps and would align with the focus of the exam.
upvoted 1 times

xRiot007 1 year, 2 months ago
"PATs are typically used to authenticate users or services to Azure DevOps resources, and are not specifically designed for registering self-hosted agents. " - Wrong. That's exactly one of the use cases of PATs. https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/linux-agent?view=azure-devops . As for SSH, they are used to authenticate to 3rd party services, like GitHub, so that the agent can clone repos. So, to recap, you need a PAT to authenticate in DevOps and then you need a SSH for GitHub connections.
upvoted 1 times

meoukg 1 year, 10 months ago
saw it yesterday in my exam
upvoted 4 times

syu31svc 2 years, 1 month ago
Selected Answer: A
100% is A
upvoted 1 times

Govcomm 2 years, 1 month ago
PAT for registering the self-hosted agent.
upvoted 1 times

kennynelcon 2 years, 2 months ago
PAT
Tested
upvoted 1 times

Eltooth 2 years, 3 months ago
Selected Answer: A
A is the correct answer.
upvoted 3 times

UnknowMan 2 years, 4 months ago
Correct
upvoted 1 times

rdemontis 2 years, 6 months ago
Selected Answer: A
PAT is correct
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/v2-linux?view=azure-devops
upvoted 2 times

Mcphyl 1 year, 9 months ago
https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/v2-linux?view=azure-devops#authenticate-with-a-personal-access-token-pat
upvoted 2 times

shermin1 2 years, 6 months ago
Came in exam march 13....
upvoted 3 times

PlumpyTumbler 2 years, 7 months ago
Selected Answer: A
Word to PAT.

upvoted 1 times

francis6170 3 years, 2 months ago

Got this in the AZ-400 exam (June 2021).

upvoted 5 times

Question #4 *Topic 4*

You are building a Microsoft ASP.NET application that requires authentication.
You need to authenticate users by using Azure Active Directory (Azure AD).
What should you do first?

A. Assign an enterprise application to users and groups

B. Create an app registration in Azure AD

C. Configure the application to use a SAML endpoint

D. Create a new OAuth token from the application

E. Create a membership database in an Azure SQL database

Suggested Answer: *B*
Register your application to use Azure Active Directory. Registering the application means that your developers can use Azure AD to authenticate users and request access to user resources such as email, calendar, and documents.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/developer-guidance-for-integrating-applications

Community vote distribution

B (100%)

Hooters Highly Voted 3 years, 10 months ago
B. Create an app registration in Azure AD
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-v2-aspnet-webapp
upvoted 25 times

francis6170 Highly Voted 3 years, 2 months ago
Got this in the AZ-400 exam (June 2021).
upvoted 14 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: B
B. Create an app registration in Azure AD
upvoted 1 times

vsvaid 9 months ago
Selected Answer: B
Agree with B
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: B
Create an App registration in AZ AD
upvoted 2 times

zellck 1 year, 3 months ago
Selected Answer: B
B is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/develop/application-model
For an identity provider to know that a user has access to a particular app, both the user and the application must be registered with the identity provider. When you register your application with Azure Active Directory (Azure AD), you're providing an identity configuration for your application that allows it to integrate with the Microsoft identity platform.
upvoted 1 times

DGladiator 1 year, 4 months ago
B. confirmed by GPT4
upvoted 2 times

surensaluka 1 year, 7 months ago

Selected Answer: B

This question came today (2023-02-14)

upvoted 3 times

syu31svc 2 years, 1 month ago

Selected Answer: B

https://docs.microsoft.com/en-us/azure/active-directory/develop/web-app-quickstart?pivots=devlang-aspnet

Step 1: Register your application
Sign in to the Azure portal.
If you have access to multiple tenants, use the Directory + subscription filter in the top menu to switch to the tenant in which you want to register the application.
Search for and select Azure Active Directory.
Under Manage, select App registrations > New registration.

Answer is B

upvoted 2 times

Govcomm 2 years, 1 month ago

Create an app for the registration and service principal

upvoted 2 times

Cheehp 2 years, 5 months ago

Selected during exam.
B. Create an app registration in Azure AD

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: B

correct
https://docs.microsoft.com/en-us/azure/active-directory/develop/web-app-quickstart?pivots=devlang-aspnet

upvoted 2 times

sujitwarrier11 2 years, 7 months ago

Selected Answer: B

create app registration

upvoted 2 times

Kalaismile06 3 years, 1 month ago

Got this question in July exam(AZ-400). Ans is B

upvoted 2 times

goatlord 3 years, 1 month ago

B for Big Time Correct.

upvoted 3 times

Ash111 3 years, 3 months ago

B is the correct ans

upvoted 2 times

kumardeb 3 years, 10 months ago

B. Create an app registration in Azure AD

upvoted 3 times

Question #5 *Topic 4*

You have an Azure DevOps organization named Contoso.
You need to recommend an authentication mechanism that meets the following requirements:
➪ Supports authentication from Git
➪ Minimizes the need to provide credentials during authentication
What should you recommend?

A. personal access tokens (PATs) in Azure DevOps

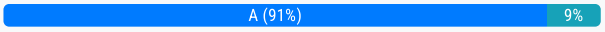
B. Alternate credentials in Azure DevOps

C. user accounts in Azure Active Directory (Azure AD)

D. managed identities in Azure Active Directory (Azure AD)

Suggested Answer: *A*
Personal access tokens (PATs) give you access to Azure DevOps and Team Foundation Server (TFS), without using your username and password directly.
These tokens have an expiration date from when they're created. You can restrict the scope of the data they can access. Use PATs to authenticate if you don't already have SSH keys set up on your system or if you need to restrict the permissions that are granted by the credential.
Incorrect Answers:
B: Azure DevOps no longer supports Alternate Credentials authentication since the beginning of March 2, 2020. If you're still using Alternate Credentials, we
[Microsoft] strongly encourage you to switch to a more secure authentication method (for example, personal access tokens).
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/git/auth-overview

Community vote distribution



SriLen Highly Voted 3 years, 7 months ago
A. Correct Answer
upvoted 20 times

goatlord Highly Voted 3 years, 1 month ago
Why is this not D?
upvoted 5 times

FoxDumpz 2 years, 12 months ago
support from git
upvoted 5 times

Miten94 Most Recent 2 months, 3 weeks ago
Came in Exam June 23, 2024
upvoted 3 times

vsvaid 9 months ago
Selected Answer: A
Personal Access Token
upvoted 1 times

Rod_DA 11 months, 4 weeks ago
Selected Answer: C
When authenticating with PAT you still need to pass credentials. Letter C, once you are logged in, you can access git (Azure Repos) without passing credentials (minimizing authentication efforts)
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: A
Provided solution is correct

upvoted 1 times

DGladiator 1 year, 4 months ago

A. confirmed by gpt4

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: A

100% is A

upvoted 3 times

Govcomm 2 years, 1 month ago

PAT Personal Access Token

upvoted 2 times

UnknowMan 2 years, 4 months ago

Selected Answer: A

Correct

upvoted 2 times

rdemontis 2 years, 6 months ago

Selected Answer: A

correct answer and explanation

upvoted 3 times

mobrockers 3 years, 1 month ago

Answer C provides the best chance the user will not have to provide authentication, because the windows login user can be used to perform SSO on git with azure devops. Nowhere in the question does it state that it's an automated process that should access git. I think the answer should be C.

upvoted 3 times

GigaCaster 2 years, 10 months ago

The question states to minimize the need to provide credentials.

upvoted 2 times

resonant 1 year, 2 months ago

You don't provide credentials with SSO if you are already signed in, even if in another application that also uses SSO. As @mobrockers says, the question doesn't say anywhere if the process is going to be automated or not, and giving a PAT is giving credentials because I think PATs are another form of credentials and with SSO you wouldn't have to provide anything.

upvoted 1 times

resonant 1 year, 2 months ago

Forgot to mention that SSO with git is possible thanks to git-credential-manager, and that it supports, among others, Azure Repos.

upvoted 1 times

resonant 1 year, 2 months ago

Ok I just read the link that the examtopics's answer provides and apparently git-credential-manager basically creates a PAT under the hood.

https://learn.microsoft.com/en-us/azure/devops/repos/git/auth-overview?view=azure-devops#use-credential-managers-to-generate-tokens

"The Git Credential Manager is an optional tool that makes it easy to create PATs when you're working with Azure Repos."

"PATs are generated on demand when you have the credential manager installed. The credential manager creates the token in Azure DevOps and saves it locally for use with the Git command line or other client."

With all of this said, I think SSH would be a better option for this and if this option was available as a choice in the question I'd choose this instead.

upvoted 1 times

V_Ramon 3 years, 1 month ago

this question came out today, July 28, 2021

upvoted 3 times

Question #6 *Topic 4*

You have an application that consists of several Azure App Service web apps and Azure functions.
You need to assess the security of the web apps and the functions.
Which Azure feature can you use to provide a recommendation for the security of the application?

A. Security & Compliance in Azure Log Analytics

B. Resource health in Azure Service Health

C. Smart Detection in Azure Application Insights

D. Compute & apps in Azure Security Center

Suggested Answer: *D*
Monitor compute and app services: Compute & apps include the App Services tab, which App services: list of your App service environments and current security state of each.

Recommendations -
This section has a set of recommendations for each VM and computer, web and worker roles, Azure App Service Web Apps, and Azure App Service Environment that Security Center monitors. The first column lists the recommendation. The second column shows the total number of resources that are affected by that recommendation. The third column shows the severity of the issue.
Incorrect Answers:
C: Smart Detection automatically warns you of potential performance problems, not security problems in your web application.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/proactive-diagnostics

Community vote distribution
D (100%)

PM2 Highly Voted 4 years ago
Correct Verified
upvoted 17 times

UrbanRellik 4 months ago
https://azure.microsoft.com/en-us/blog/protecting-windows-virtual-desktop-environments-with-azure-security-center/
upvoted 1 times

hajurbau Most Recent 3 months ago
Selected Answer: D
Azure security center is now called Microsoft defender for cloud.
upvoted 1 times

hajurbau 2 months, 1 week ago
Agreed!
upvoted 1 times

ozbonny 6 months, 3 weeks ago
Selected Answer: D
Compute & apps in Azure Security Center
upvoted 2 times

vsvaid 9 months ago
Selected Answer: D
D is Correct
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: D
https://docs.microsoft.com/en-us/azure/defender-for-cloud/security-policy-concept

Answer is D (Microsoft Defender for Cloud is the new name for Azure Security Center)

upvoted 4 times

Govcomm 2 years, 1 month ago

Computer & Apps in the Azure Security Center / Microsoft Defender for Cloud

upvoted 2 times

Eltooth 2 years, 3 months ago

Selected Answer: D

D is correct answer. Was in exam and scored 100% on this section.

upvoted 4 times

UnknowMan 2 years, 4 months ago

Correct (Azure Security Center is called Microsoft Defender for Cloud now)

upvoted 2 times

rdemontis 2 years, 6 months ago

Selected Answer: D

correct even if now Azure Security Center is called Microsoft Defender for Cloud

https://docs.microsoft.com/en-us/azure/defender-for-cloud/asset-inventory

upvoted 3 times

sujitwarrier11 2 years, 7 months ago

Selected Answer: D

Security center

upvoted 2 times

shuakwe 2 years, 7 months ago

Azure Security Center is now called Defender for Cloud

https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction

upvoted 3 times

eddy_040695 3 years ago

Correct

upvoted 1 times

Anjosh 3 years, 1 month ago

Correctina

upvoted 1 times

Miles19 3 years, 5 months ago

Coretto

upvoted 1 times

RKS 3 years, 7 months ago

Correct!!!

upvoted 2 times

swati17 3 years, 10 months ago

correct.

upvoted 3 times

CristianN 4 years ago

https://docs.microsoft.com/en-us/azure/security-center/security-center-virtual-machine-protection

upvoted 3 times

Question #7 *Topic 4*

Your company has a project in Azure DevOps for a new web application.
The company identifies security as one of the highest priorities.
You need to recommend a solution to minimize the likelihood that infrastructure credentials will be leaked.
What should you recommend?

A. Add a Run Inline Azure PowerShell task to the pipeline.

B. Add a PowerShell task to the pipeline and run Set-AzureKeyVaultSecret.

C. Add an Azure Key Vault task to the pipeline.

D. Add Azure Key Vault references to Azure Resource Manger templates.

Suggested Answer: *B*
Azure Key Vault provides a way to securely store credentials and other keys and secrets.
The Set-AzureKeyVaultSecret cmdlet creates or updates a secret in a key vault in Azure Key Vault.
Reference:
https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/set-azurekeyvaultsecret

Community vote distribution
C (57%) D (43%)

silverdeath Highly Voted 4 years, 5 months ago
D is correct and needed, so the correct answer should be D
upvoted 53 times

jay158 2 years, 5 months ago
What is web app is deployed using Terraform, it is not specified that deployment is using ARM Templates?
upvoted 6 times

NandoRU777 1 year, 7 months ago
In terraform you can reference to Azure Key Vault secrets too and inject it in the entire Terreform infrastructure deployment code
upvoted 1 times

Tyler2023 1 year ago
This is a Microsoft related certification, there is small number of question that requires third party tools, so always assume that we are using Microsoft Azure tools like ARM and Bicep
upvoted 3 times

artisticcheese Highly Voted 4 years, 9 months ago
Correct answer is C. This is the task to retreive Keyvault secrets to use in following tasks
upvoted 28 times

NKnab 4 years, 1 month ago
https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/deploy/azure-key-vault?view=azure-devops
upvoted 2 times

Yanzhi 4 years, 9 months ago
D is more "correct" than C, because the protection object is infra's credential, it may or may not used in pipeline.
upvoted 73 times

hart232 4 years, 3 months ago
.....Assuming ARM is used for deploying infrastructure.
upvoted 5 times

Fred64 4 years, 3 months ago
The pbl with C is that we will inject secrets into parameters. They can later be read in the deployent blade in the portal
upvoted 5 times

icedog 1 year, 2 months ago
not if the parameter type is securestring, if it's anything else then yes it can be read
upvoted 1 times

TosO 4 years, 5 months ago
Correct
upvoted 10 times

silverdeath 4 years, 4 months ago
yes, correct
upvoted 3 times

Tyler2023 1 year ago
The Set-AzKeyVaultSecret cmdlet creates or updates a secret in a key vault in Azure Key Vault. If the secret does not exist, this cmdlet creates it. If the secret already exists, this cmdlet creates a new version of that secret.

You need to use the Get-AzKeyVaultSecret cmdlet gets secrets in a key vault. This cmdlet gets a specific secret or all the secrets in a key vault.

ANSWER is D:

https://learn.microsoft.com/en-us/powershell/module/az.keyvault/set-azkeyvaultsecret?view=azps-10.2.0
upvoted 2 times

ozbonny 6 months, 3 weeks ago
but it stores credentials within scripts so it poses a security risk.
upvoted 1 times

hajurbau Most Recent 3 months ago
Selected Answer: C
Going with C assuming adding kv task in ado pipeline
upvoted 1 times

hajurbau 3 months, 1 week ago
Selected Answer: C
I am going with C assuming I am adding keyvault task in the ado pipeline.
upvoted 1 times

isaurabhgoyal 4 months, 2 weeks ago
Selected Answer: C
Option D, adding Azure Key Vault references to Azure Resource Manager templates, is a valid approach for securely accessing credentials and other sensitive information in your infrastructure deployment. However, it is more focused on managing secrets within your infrastructure code rather than in your CI/CD pipeline.

For the specific scenario of minimizing the likelihood of infrastructure credentials being leaked in an Azure DevOps pipeline, using an Azure Key Vault task directly in the pipeline (Option C) is a more direct and secure approach. This allows you to retrieve secrets from Azure Key Vault at runtime without exposing them in your pipeline configuration.

So the ANS is C
upvoted 3 times

4bd3116 4 months, 3 weeks ago
Selected Answer: C
By using an Azure Key Vault task in your pipeline, you can retrieve secrets during runtime without exposing them in your code or configuration files.
upvoted 1 times

chloaus 5 months, 1 week ago
The question is referring to infrastructure credentials.
Instead of putting a secure value (like a password) directly in your template or parameter file, you can retrieve the value from an Azure Key Vault during a deployment. You retrieve the value by referencing the key vault and secret in your parameter file. The value is never exposed because you only reference its key vault ID.
https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli
upvoted 1 times

ozbonny 6 months, 3 weeks ago
https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli

upvoted 1 times

ozbonny 6 months, 3 weeks ago

C. Add an Azure Key Vault task to the pipeline.

upvoted 1 times

saket051985 7 months, 3 weeks ago

C. Add an Azure Key Vault task to the pipeline.

By using Azure Key Vault tasks, you can securely store and retrieve secrets in Azure Key Vault during your build or release process, reducing the exposure of sensitive information like credentials in your pipelines.

Option D (Add Azure Key Vault references to Azure Resource Manager templates) is also a good practice, but it may not directly address the concern of credentials leaking during the pipeline execution. It's more about securely referencing secrets during infrastructure deployment.

Therefore, the correct answer is C

upvoted 1 times

vsvaid 8 months, 2 weeks ago

Selected Answer: C

I think C as this task is only for reteiving passwords securly. Can be done with D as well but for C is better choice

upvoted 1 times

_alex_123 10 months, 3 weeks ago

D as it is more secure than KV task:"The task can be used to fetch the latest values of all or a subset of secrets from the vault and set them as variables that can be used in subsequent tasks of a pipeline. " With ARM template/parameter file a particular KV secret is referred and that KV secret value is only "visible" for that particular ARM or AzureCLI task

upvoted 2 times

Jrcondado80 11 months ago

Selected Answer: C

Correct answer is C

upvoted 1 times

krzychu3000 1 year, 1 month ago

Selected Answer: C

KV task

upvoted 2 times

stai 1 year, 1 month ago

Correct answer is C.

upvoted 1 times

flafernan 1 year, 1 month ago

B, C, D - Regarding which option is the right one, it is important to remember that there is no one-size-fits-all answer, as each project may have specific needs. The recommended option will depend on the project context, security requirements, and team preferences.

Microsoft's official solution, "Add a PowerShell task to the pipeline and run Set-AzureKeyVaultSecret", is a good choice because it offers a high level of control and flexibility. However, the other options may also be equally valid, depending on the details of the project.

upvoted 2 times

vector_bco 10 months, 3 weeks ago

your kv have a secret named sqlPassword with the value 123456

when you will run Set-AzureKeyVault command you will not get 123456, so selected answer in 146% incorrect

There 2 options here C and D with some advantages and disadvantages for both

upvoted 1 times

xRiot007 1 year, 2 months ago

You want credentials not to be leaked. This means they CANNOT be anywhere in your infrastructure scripts of pipeline. To do this, you will add Azure Key Vault key references. At runtime, the pipeline will ask the Vault for values and pass them immediately to the infrastructure scripts.

upvoted 1 times

xRiot007 1 year, 2 months ago

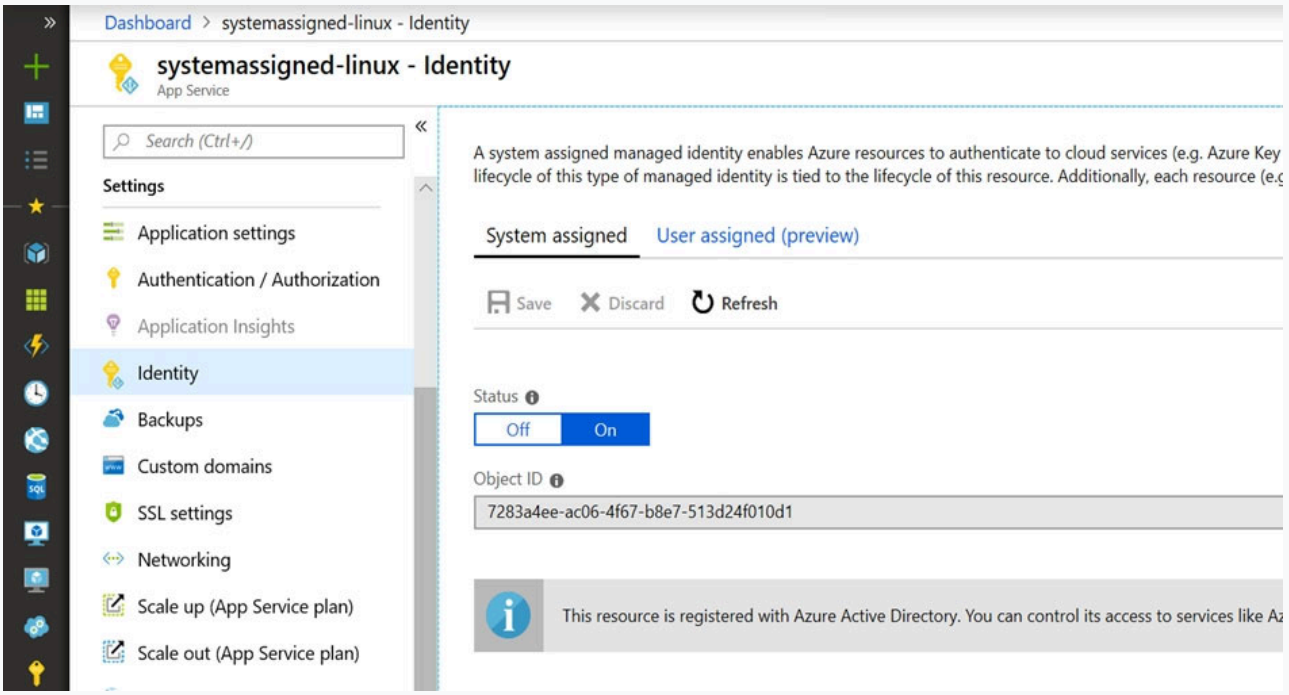
To sum it up, answer is D.

upvoted 2 times

Question #8 *Topic 4*

SIMULATION -
You need to ensure that an Azure web app named az400-123456789-main can retrieve secrets from an Azure key vault named az400-123456789-kv1 by using a system managed identity.
The solution must use the principle of least privilege.
To complete this task, sign in to the Microsoft Azure portal.

Suggested Answer: *See explanation below.*
1. In Azure portal navigate to the az400-123456789-main app.
2. Scroll down to the Settings group in the left navigation.
3. Select Managed identity.
4. Within the System assigned tab, switch Status to On. Click Save.



Reference:
https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity

Rams_84zO6n Highly Voted 1 year, 6 months ago
web app must retrieve the secrets from KV.
The solution stops short of that. It only create MI. It is missing the next step. The next step is go to KeyVault, access policies - click create, select permissions, select web app MI, click next and save. Do you agree?
upvoted 14 times

mshin 1 year, 6 months ago
Look at the 'Configure the web app to connect to Key Vault' section.
It should clear up the doubts on how to setup az keyvault for web apps.
KeyVault --> Access policies (Az Portal or Powershell) --> Select perms --> Select Object ID (Web app managed identity object)
https://learn.microsoft.com/en-us/azure/key-vault/general/tutorial-net-create-vault-azure-web-app
upvoted 2 times

NgCK Highly Voted 10 months, 3 weeks ago
1. Turn on System assigned managed identity for az400-123456789-main.

(Based on role-based access control (RBAC) instead of access policy)
2. At the key vault az400-123456789-kv1, go to:
Access control (IAM) >
Add role assignment > Choose Key Vault Secrets User > choose assign access to managed identity > Click select members > Select the app system managed identity
upvoted 5 times

phantom31 3 months, 3 weeks ago
This is the way to do this in May 2024
upvoted 5 times

chakanirban Most Recent 2 months, 3 weeks ago
NO LAB on 6/21 - 9 am IST -
1 Case study , 6 new Q

1 YES NO series was new - 3 Q - I answered all No , because 2 will No and 1 Y
JOB A depends JOB B
JOB B on JOB C
JOB C on JOB D

who is dependent , who can run parallel
3 yes/ no
upvoted 2 times

ozbonny 6 months, 3 weeks ago
I followed the next steps in my own subscription:
Create a web app
set the identity in on, copy the identity id
create a keyvault
enable access policies because RBAC are set as default (you need to be user access admin or owner)
go to add a new access policy
select the permissions
set the app identity id by pasting the identity id in the search box
click on review and create and that's all
upvoted 3 times

meoukg 1 year, 10 months ago
I saw this question in the lab along with other 7 questions
upvoted 4 times

eliisiita1 1 year, 10 months ago
did you do the exam online?
upvoted 4 times

xda 7 months, 2 weeks ago
can comfirm the same (January 2024)
upvoted 2 times

Question #9 *Topic 4*

You create a Microsoft ASP.NET Core application.
You plan to use Azure Key Vault to provide secrets to the application as configuration data.
You need to create a Key Vault access policy to assign secret permissions to the application. The solution must use the principle of least privilege.
Which secret permissions should you use?

A. List only

B. Get only

C. Get and List

Suggested Answer: *B*
Application data plane permissions:
➪ Keys: sign
➪ Secrets: get
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

Community vote distribution

ttm_19 Highly Voted 4 years, 3 months ago
Get only is enough. Tested!
upvoted 63 times

xRiot007 1 year, 2 months ago
Let's not be more catholic than the Pope, as the saying does. Get and List are both read only and to be used in the pipeline, where Get will fetch a specific key-value entry and List will fetch all entries : https://azuredevopslabs.com/labs/vstsextend/azurekeyvault/
upvoted 4 times

Kent_020 11 months, 1 week ago
Thank you!
upvoted 1 times

hipana8796 4 years, 2 months ago
I think get alone would fail if you try to obtain all secrets from the KV.
upvoted 2 times

ttm_19 4 years, 2 months ago
If you need to read/provide to the webapp a list of secrets at once - yes, it will need List as well. But do we need to provide such list, or just a specific secret on request?
Tested with .netcore webapp (3.1), deployed to an App Service, retrieving values from 2 keyvault secrets. Values are defined as Application Settings in the App Svc, with a reference to the keyvault: @Microsoft.KeyVault(SecretUri= {uri to the secret here}) . And it worked with only GET permission!
upvoted 17 times

d0bermannn 3 years ago
no way, we must to go step by step our honorabe coder stars to knew their exactly rights in system
upvoted 1 times

ttm_19 4 years, 2 months ago
the scenario described by me is the most common - having a number settings and retrieving their values. Example:
KeyVaultSecret secret1 = client.GetSecret("mySecret1");
KeyVaultSecret secret2 = client.GetSecret("mySecret2");
In fact, in the SecretsClient class (https://docs.microsoft.com/en-us/dotnet/api/azure.security.keyvault.secrets.secretclient?view=azure-dotnet) there is no method for listing available secrets (only the deleted ones).
upvoted 4 times

xRiot007 1 year, 2 months ago

Just to make myself undetstood. If a value should not be used by an APP, it should not exist in that Key Vault to begin with. We use a Key vault to secure values not from apps, but from malicious human actors.
upvoted 2 times

kaikailiang Highly Voted 4 years, 3 months ago
I think "Get and List" is the correct answer.
upvoted 9 times

prashantjoge 2 years, 5 months ago
When you want to access secrets:

Ensure the Azure service connection has at least Get and List permissions on the vault. You can set these permissions in the Azure porta
upvoted 1 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: C
I think get and list
C
upvoted 1 times

vsvaid 9 months ago
Selected Answer: B
I think B as it is case of least privilege. No need for list
upvoted 1 times

thuvh 10 months, 1 week ago
Selected Answer: C
Get and List: https://learn.microsoft.com/en-us/aspnet/core/security/key-vault-configuration?view=aspnetcore-7.0
upvoted 1 times

Tyler2023 1 year ago
The "get" permission is enough

Get: This permission allows the application to retrieve (read) secrets from the Key Vault. It's typically the most basic permission you would grant to an application that needs access to secrets.

List: This permission allows the application to list the names of secrets in the Key Vault. It doesn't provide access to the values of the secrets, only the names. You might need this permission if your application needs to discover the names of secrets dynamically.
upvoted 4 times

ieboaix 1 year, 1 month ago
C. Both Get and List are read-only and there is nothing less that read-only. based on https://learn.microsoft.com/en-us/answers/questions/133948/list-and-get-key-operations-in-azure-key-vault. I didnt see any less secure for list operation.
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: B
Get only
upvoted 3 times

flafernan 1 year, 1 month ago
B:
within least privilege rules, by granting “Get only” permission, application will only be able to retrieve values of secrets from Azure Key Vault, but will not be allowed to list all secrets in Key Vault. This ensures that the application only has access to the specific secrets it needs, without excessive or necessary access to other secrets.
upvoted 2 times

icedog 1 year, 2 months ago
Selected Answer: B
Well I use Get only on our platform
B. is the correct answer
upvoted 2 times

zellck 1 year, 3 months ago
Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/devops/pipelines/release/azure-key-vault?view=azure-devops&tabs=yaml#set-up-azure-key-vault-access-policies
For Secret permissions, select Get and List.
upvoted 1 times

zellck 1 year, 3 months ago
C is the answer.

https://learn.microsoft.com/en-us/azure/devops/pipelines/release/azure-key-vault?view=azure-devops&tabs=yaml#set-up-azure-key-vault-access-policies
For Secret permissions, select Get and List.
upvoted 1 times

318touring 1 year, 4 months ago
Selected Answer: C
Get and List

1. Tested using this tutorial: https://azuredevopslabs.com/labs/vstsextend/azurekeyvault/
2. Set Access Policy tin KV for the SP to Get only. The release returned this error: "does not have secrets list permission on key vault 'az400test;location=australiaeast'"
3. Added 'List' for the Access Policy for the SP, and the Release finished successfully
upvoted 3 times

Pipek 1 year, 5 months ago
Selected Answer: B
Get only !
upvoted 2 times

AlexLiourtas 1 year, 6 months ago
you cant get if you cannot list
upvoted 2 times

AlexeyG 1 year, 6 months ago
got this in 02 March 2023 exams. scored 870 marks.
upvoted 3 times

nikipediaa 1 year, 7 months ago
Got this Feb 2023
upvoted 1 times

Yunus 1 year, 7 months ago
What's the answer ?
upvoted 1 times

DRAG DROP -

Your company has a project in Azure DevOps.

You plan to create a release pipeline that will deploy resources by using Azure Resource Manager templates. The templates will reference secrets stored in Azure

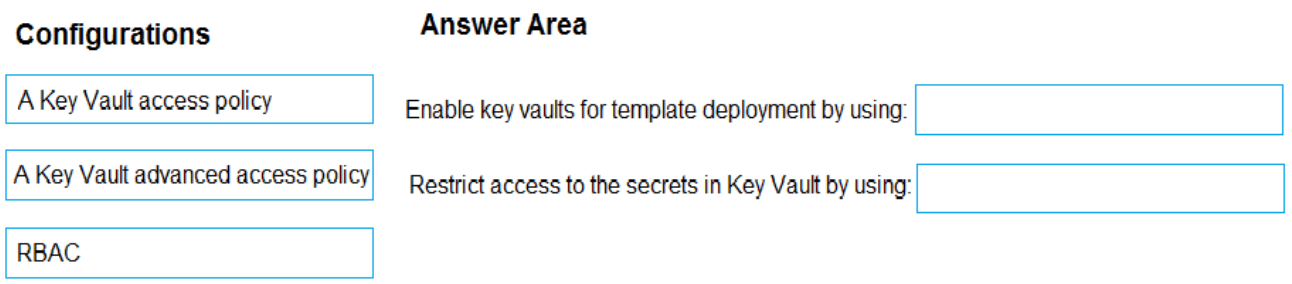
Key Vault.

You need to recommend a solution for accessing the secrets stored in the key vault during deployments. The solution must use the principle of least privilege.

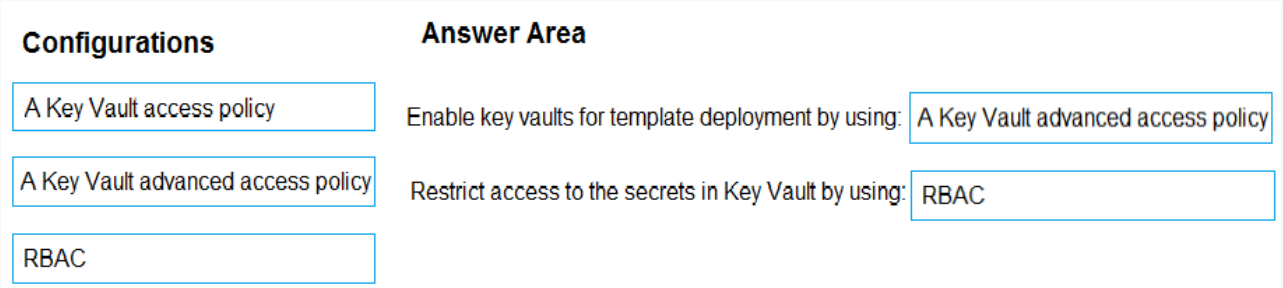
What should you include in the recommendation? To answer, drag the appropriate configurations to the correct targets. Each configuration may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

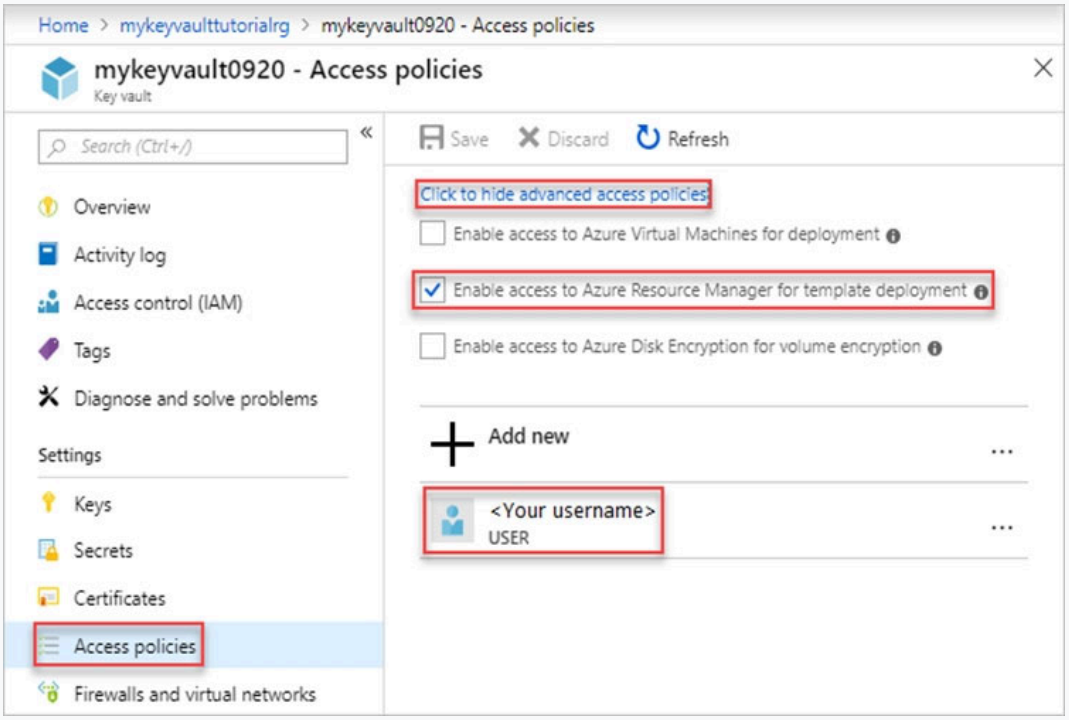
Select and Place:



Suggested Answer:



Box 1: A key Vault advanced access policy



Box 2: RBAC -

Management plane access control uses RBAC.

The management plane consists of operations that affect the key vault itself, such as:

➪ Creating or deleting a key vault.

➩ Getting a list of vaults in a subscription.
➩ Retrieving Key Vault properties (such as SKU and tags).
➩ Setting Key Vault access policies that control user and application access to keys and secrets.
Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-tutorial-use-key-vault

Kazillius Highly Voted 3 years, 2 months ago
Answer should be:
1) A Key Vault access policy
2) A Key Vault access policy
upvoted 48 times

rfox321 2 years, 11 months ago
Why is this the correct answer? Link?
upvoted 4 times

rdemontis 2 years, 6 months ago
"To enable the template to retrieve the secret, you must enable an access policy called Enable access to Azure Resource Manager for template deployment for the key vault. This policy is enabled in the template"

Please look at the link below (Important section)

https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/template-tutorial-use-key-vault#prepare-a-key-vault

The answer provided by exam topic is really outdated. The section Advanced access policy has been removed from years and now, as you can easily test in the portal, the only thing to do for either the question is to create an access policy. Specifically, to enable key vaults for template deployment you need only to flag the proper checkbox
upvoted 4 times

rdemontis 2 years, 5 months ago
However, if "Advanced access policy" were to be present as an option on the exam I would consider using it for the first box. Because an obsolete answer also suggests that the question is obsolete.
upvoted 2 times

catfood 1 year, 1 month ago
access policies aren't needed if the user is deploying a template that retrieves a secret

https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli

Outdated question IMHO, going to ignore it.
upvoted 1 times

awron_durat 2 years, 7 months ago
I think this question is just very out of date. I checked KV and they don't even have an advanced access policy section anymore.
upvoted 15 times

ParkXD 1 year, 6 months ago
agree, now it is "resource access" in the Access configuration
upvoted 2 times

prashantjoge 2 years, 5 months ago
Advanced policy is needed for template deployment
key vault policy since rbac is needed for managing the keyvault itself
upvoted 1 times

mshin 1 year, 6 months ago
1) Advanced Access Policy
Note, this option is now replaced by 'Access Configurations'.
Portal --> Key vault --> Access Configuration --> Enable Az Resource Manager for template deployment option

2) Key Vault Access policies
Role-Based Access Control (RBAC) are used for managing Azure Active Directory (AAD) users, groups, and applications at a management

plane level (assigning roles, creating custom roles with specific perms),
Whereas Access Policies are used for managing Key Vault data plane operations, such as read, write, and delete secrets.

So Access Policies are specific to Azure Key Vault and are used to manage access to the secrets and keys stored within it.

As mentioned in the comments below a good rule of thumb is to remember:
- access to the key vault could be provided by RBAC
- access to the keys/secrets in key vault could be provided by access policy
- access for a period of time can be provided by SAS.
upvoted 6 times

fkaracan 1 year, 7 months ago
who are you and why should we trust you without giving explanation :D
upvoted 5 times

sv_26 Highly Voted 3 years, 2 months ago
answer should be
A key vault access policy
RABC
upvoted 29 times

rfox321 2 years, 11 months ago
Links for proof please?
upvoted 3 times

CompetentNinja 2 years, 5 months ago
Try to enable it in portal and you will se your self. In new version there is no "advanced"
upvoted 2 times

Skankhunt Most Recent 1 month, 3 weeks ago
Old question, the correct answer now would be:
Key Vault Access configuration. Here you can enable "Azure Resource Manager for template deployment".

RBAC
upvoted 1 times

arr73 4 months, 2 weeks ago
I think that question is old, and the response has changed. Now I think it should be:
Slot1: RBAC
Slot2: RBAC

Explanation:
Micorosft recommends to migrate from access-policies (legacy) to RBAC. See provived link, that says:
Azure Key Vault offers two authorization systems: Azure role-based access control (Azure RBAC), which operates on Azure's control and data planes, and the access policy model, which operates on the data plane alone. Azure RBAC is the recommended authorization system for the Azure Key Vault data plane

https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-access-policy#data-plane-access-control-recommendation
upvoted 1 times

arr73 2 months, 2 weeks ago
I was wrong: it's access policy, as rdemontis explained. Sorry for the mistake.
upvoted 1 times

chloaus 5 months, 1 week ago
Correct Answer: 3, 1
The access policies aren't needed if the user is deploying a template that retrieves a secret. Add a user to the access policies only if the user needs to work directly with the secrets.
The user who deploys the template must have the Microsoft.KeyVault/vaults/deploy/action permission for the scope of the resource group and key vault.
Recommendations for controlling access to your vault are as follows:
Lock down access to your subscription, resource group, and key vaults using role-based access control (RBAC).
Restrict network access with Private Link, firewall and virtual networks

https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli
https://learn.microsoft.com/en-us/azure/key-vault/general/best-practices
upvoted 1 times

yana_b 10 months, 3 weeks ago
1. Access configurations under Settings on the Key vault blade itself
2. Access to the data in the KV itself => Data plane and here we can chose btw. Access Policy and Key Vault
upvoted 2 times

yana_b 1 year, 1 month ago
This questions is a bit outdated.
The newer version split it to 2 separate questions asking for restricting access to:
- delete the key vault => RBAC
- the secrets stored in the key vault? => key access policy
upvoted 15 times

WH16 1 year ago
Yes, it was on exam 2023-09-06, went with answers above and scored 933.
upvoted 4 times

renzoku 1 year, 2 months ago
1. Access Policies
Fine-grained approach for controlling access to the secrets in Azure Key Vault.

2. RBAC
Commonly used for managing access to Azure resources(e.g. Key Vault).
upvoted 4 times

Pipek 1 year, 5 months ago
1) Enable key vaults for template deployment: RBAC
https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli
The access policies aren't needed if the user is deploying a template that retrieves a secret. Add a user to the access policies only if the user needs to work directly with the secrets. The deployment permissions are defined in the next section.
2) Access policy
upvoted 1 times

AzureJobsTillRetire 1 year, 8 months ago
As a rule of thumb, access to the key vault could be provided by RBAC, access to the keys/secretes in key vault could be provided by access policy, and access for a period of time can be provided by SAS. I have used this rule of thumb across a few Azure exams (AZ-104, AZ-305, AZ-700, AZ-500) and it never fails me. I hope it works in AZ-400 as well. It must be some very specific reasons that the rule does not apply.
upvoted 14 times

rikininetysix 1 year, 8 months ago
Seems like the answer should be -
1) A Key Vault access policy
2)RBAC

https://learn.microsoft.com/en-us/answers/questions/370371/restrict-access-to-the-secrets-in-the-key-vault-ar.html

Access to vaults takes place through two interfaces or planes.

Management plane is controlled via RBAC to manage Key Vault itself. Operations that can be controlled are:
> Create, read, update, and delete key vaults
> Set Key Vault access policies
> Set Key Vault tags

Data plane is controlled via Access Policies to allows you to work with the data stored in a key vault. Operations that can be controlled are:
> Keys: encrypt, decrypt, wrapKey, unwrapKey, sign, verify, get, list, create, update, import, delete, recover, backup, restore, purge
> Certificates: managecontacts, getissuers, listissuers, setissuers, deleteissuers, manageissuers, get, list, create, import, update, delete, recover, backup, restore, purge
> Secrets: get, list, set, delete,recover, backup, restore, purge

upvoted 3 times

rikininetysix 1 year, 8 months ago

Sorry for the mistake, the answer given is entirely correct, first answer would be the A Key Vault advanced access policy and second one would be RBAC.

upvoted 1 times

Rachid 1 year, 9 months ago

The first option has to be enabled in KV/ Access Configuration /Resource access

The Resource access
Choose among the following options to grant access to specific resource types
Azure Virtual Machines for deployment
> Azure Resource Manager for template deployment
Azure Disk Encryption for volume encryption

upvoted 3 times

hebertpena88 1 year, 11 months ago

Today's answer is:
1. Access Policy
2. Access Configuration -- Here you can setup permissions for VMs

upvoted 2 times

Akssssh 1 year, 11 months ago

Both should be - a key vault access policy
https://learn.microsoft.com/en-us/answers/questions/370371/restrict-access-to-the-secrets-in-the-key-vault-ar.html

https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/template-tutorial-use-key-vault

upvoted 2 times

Atos 2 years ago

A Key Vault access policy - an access policy is only way to setup this option
RBAC - Only way to restrict access would be a permission model, role based is only option, so rather obvious.

upvoted 3 times

Def21 2 years ago

Correct answer is:
1) A key vault access policy (which is called "advanced" setting in warning messages)
2) RBAC

The answer options are out-of-date.

Explanation:
Currently in the portal "Access configuration" you can select "Azure role-based access control" or "Vault access policy". Independent of this selection, there is a possibility to select "Azure Resource Manager for template deployment". There is no word "Advanced" anywhere. However, in warning messages, the last option is described as an advanced access policy.

upvoted 4 times

Narender_892 2 years ago

1. Answer didn't give in the options. It should be an Access configuration blade in the Key vault
2. A Key Vault access policy
2.

upvoted 2 times

Question #11 *Topic 4*

DRAG DROP -

You need to configure access to Azure DevOps agent pools to meet the following requirements:

➩ Use a project agent pool when authoring build or release pipelines.

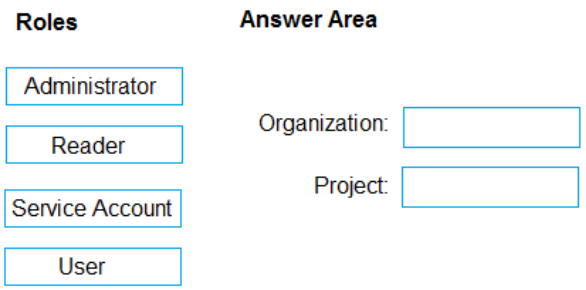
➩ View the agent pool and agents of the organization.

➩ Use the principle of least privilege.

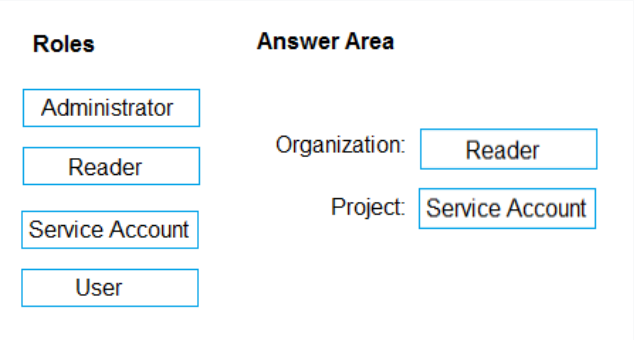
Which role memberships are required for the Azure DevOps organization and the project? To answer, drag the appropriate role memberships to the correct targets. Each role membership may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested Answer:



Box 1: Reader -

Members of the Reader role can view the organization agent pool as well as agents. You typically use this to add operators that are responsible for monitoring the agents and their health.

Box 2: Service account -

Members of the Service account role can use the organization agent pool to create a project agent pool in a project. If you follow the guidelines above for creating new project agent pools, you typically do not have to add any members here.

Incorrect Answers:

In addition to all the permissions given the Reader and the Service Account role, members of the administrator role can register or unregister agents from the organization agent pool. They can also refer to the organization agent pool when creating a project agent pool in a project. Finally, they can also manage membership for all roles of the organization agent pool. The user that created the organization agent pool is automatically added to the Administrator role for that pool.

Reference:

https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/pools-queues

TosO Highly Voted 4 years, 5 months ago

Organization -> Reader

Project -> User

upvoted 177 times

Art3 2 years, 8 months ago

Correct! reader, User.

upvoted 3 times

NKnab 4 years, 1 month ago

This one is the correct answer.

upvoted 6 times

rdemontis 2 years, 5 months ago

you are right. You can read the article below for more details:

https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/pools-queues?view=azure-devops&tabs=yaml%2Cbrowser#security

upvoted 4 times

rdemontis 2 years, 5 months ago

Also see this article for best explanation

https://docs.microsoft.com/en-us/azure/devops/organizations/security/about-security-roles?view=azure-devops

upvoted 5 times

[Removed] Highly Voted 4 years, 6 months ago

I think the Project level access should be User in this scenario

upvoted 28 times

Miten94 Most Recent 2 months, 3 weeks ago

Came in Exam June 23, 2024

upvoted 2 times

codeguru_9777 2 months, 3 weeks ago

You had any lab/simulation in the exam?

upvoted 5 times

vsvaid 8 months, 2 weeks ago

Agree with below. There is no service account for Project security. Service account is only Organizatiuon security. https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/pools-queues?view=azure-devops&tabs=yaml%2Cbrowser

Organization -> Reader

Project -> User

upvoted 1 times

vsvaid 9 months ago

Organization- Reader

Project- User

If the user needed ability to add project agent pool then Service account at organization level.

upvoted 2 times

yana_b 1 year, 1 month ago

Correct answer is:

Organization -> reader

Project -> User

Service Account is on organization and not on Project level

https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/pools-queues?view=azure-devops&tabs=yaml%2Cbrowser#security

upvoted 1 times

renzoku 1 year, 2 months ago

Organization > Reader

Project> User

Project-level security roles

Reader: view the project agent pool

User: can use the project agent pool

Administrator: all the above operations and manage membership for all roles of the project agent pool

upvoted 2 times

Rubends 1 year, 5 months ago

Organization -> Reader

Project -> User

upvoted 3 times

formacionkiteris 1 year, 6 months ago

Project -> User
Organization -> Reader
upvoted 3 times

le129 1 year, 7 months ago
https://learn.microsoft.com/en-us/azure/devops/organizations/security/about-security-roles?view=azure-devops
upvoted 2 times

Atos 2 years ago
There is no administration work in requirements which is only thing i like about this question. Therefore the answer has to be:
Organisation - Reader
Project - User
upvoted 3 times

syu31svc 2 years, 1 month ago
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/pools-queues?view=azure-devops&tabs=yaml%2Cbrowser

"Reader Members of this role can view the agent pool as well as agents. You typically use this to add operators that are responsible for monitoring the agents and their health."

"User Members of this role can use the project agent pool when authoring pipelines."

Organization ---> Reader
Project ---> User
upvoted 4 times

UnknowMan 2 years, 4 months ago
On Project level , the Service Account, dont exist.

So the correct answer is :

Organization : Reader
Project : User
upvoted 3 times

Sara_Mo 2 years, 7 months ago
Organization -> Reader
Project -> User
Agent pool security roles, project-level
You add users to the following security roles from the project-level admin context, Agent Pools page. For information on adding and managing agent pools, see Agent pools.

TABLE 1
Role (project-level) Description
Reader Can view the pool. You typically add operators to this role that are responsible for monitoring the build and deployment jobs in that pool.
User Can view and use the pool when authoring build or release pipelines.
Creator Can create and use the pool when authoring build or release pipelines.
Administrator Can manage membership for all roles of the pool, as well as view and use the pools. The user that created a pool is automatically added to the Administrator role for that pool.
upvoted 4 times

Sara_Mo 2 years, 7 months ago
the answer is correct

Reader Can view the pool as well as agents. You typically add operators to this role that are responsible for monitoring the agents and their health.
Service Account Can use the pool to create an agent in a project. If you follow the guidelines for creating new pools, you typically do not have to add any members to this role.
Administrator Can register or unregister agents from the pool and manage membership for all pools, as well as view and create pools. They can also use the agent pool when creating an agent in a project. The system automatically adds the user that created the pool to the Administrator role for that pool.

Role Description
Reader Can only view deployment groups.
Creator Can view and create deployment groups.
User Can view and use but cannot manage or create deployment groups.
Administrator Can administer roles, manage, view and use deployment groups.
upvoted 1 times

Pankaj78 2 years, 9 months ago
Frist one is definitely not the Reader (Organization) because Members of this role can view the agent pool as well as agents. You typically use this to add operators that are responsible for monitoring the agents and their health.
upvoted 1 times

GigaCaster 2 years, 10 months ago
The issue with user at project is that the account creating the project automatically gets added to the administration area as is shown in their explanation, That's why it says service account.
upvoted 1 times

Question #12 *Topic 4*

You have a branch policy in a project in Azure DevOps. The policy requires that code always builds successfully.
You need to ensure that a specific user can always merge changes to the master branch, even if the code fails to compile. The solution must use the principle of least privilege.
What should you do?

A. Add the user to the Build Administrators group.

B. Add the user to the Project Administrators group.

C. From the Security settings of the repository, modify the access control for the user.

D. From the Security settings of the branch, modify the access control for the user.

Suggested Answer: *D*
In some cases, you need to bypass policy requirements so you can push changes to the branch directly or complete a pull request even if branch policies are not satisfied. For these situations, grant the desired permission from the previous list to a user or group. You can scope this permission to an entire project, a repo, or a single branch. Manage this permission along the with other Git permissions.
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies

Community vote distribution
D (100%)

examkid Highly Voted 4 years, 1 month ago
What a horrible scenario!
Anyway the answer is correct
upvoted 38 times

Dkijc 3 years, 10 months ago
I know, right? lol
upvoted 3 times

d0bermannn 3 years ago
yes that q is about our honorable code stars))
upvoted 1 times

ManikandaKumaran 2 years, 9 months ago
Sometimes in real time, these are valid scenarios. Some development repos won't have customer's third-party integrated software's db access. At those times developers can't compile but still need to port the changes.
upvoted 3 times

AS007 Highly Voted 4 years, 4 months ago
Correct Answer
upvoted 36 times

UrbanRellik Most Recent 4 months ago
Selected Answer: D
Although it's not recommended to allow a failed build to merge with the master branch, D will allow you to have granular control over each user's privileges.
upvoted 1 times

jmglezgz 5 months ago
Selected Answer: D
From the Security settings of the branch, modify the access control for the user.
upvoted 1 times

vsvaid 9 months ago
Selected Answer: D
Correct answer
upvoted 1 times

flafernan 1 year ago

I accepted but I don't agree with the question. The question said a specific user and I understood that it would not be the same user. Therefore, it would not be modified but rather add a new user. I also add a comment that this would not be a good practice in DevOps. Very strange question.
upvoted 1 times

yana_b 1 year, 1 month ago

Selected Answer: D

Correct answer
upvoted 1 times

xRiot007 1 year, 2 months ago

Hello Microsoft, why would you want to do this in the first place ? This is against the best practices of DevOps.
upvoted 3 times

DiligentAmoeba 1 year, 1 month ago

Agree, access should be granted to a group, of which the user is a member.
upvoted 1 times

renzoku 1 year, 2 months ago

Selected Answer: D

D: From the Security settings of the branch, modify the access control for the user.
By modifying the access control you can grant them the necessary permissions to bypass the policy in the specific branch.

Modify access control at repository scope, break the rule to use the principle of least privilege.

Build Administrators group, Project Administrators group
Grant permissions to view, managing or building pipelines and related funtionalities.
upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: D

https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-permissions?view=azure-devops

"Users with this permission are exempt from the branch policy set for the branch when completing pull requests and can opt-in to override the policies by checking Override branch policies and enable merge when completing a PR."

Answer is D
upvoted 3 times

Govcomm 2 years, 1 month ago

From the Security settings of the branch, modify the access control for the user.
upvoted 1 times

Kalaismile06 2 years, 2 months ago

Given answer is correct
upvoted 1 times

UnknowMan 2 years, 4 months ago

Because if for a specific "master branch", we user Branch security level and not Repository security level (that set for all branche)

Correct answer
upvoted 3 times

rdemontis 2 years, 6 months ago

Selected Answer: D

answer is correct as documentation provided demonstrate
upvoted 2 times

rdemontis 2 years, 5 months ago

https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops&tabs=browser#bypass-branch-policies
upvoted 1 times

Pino2012 3 years, 7 months ago

Why do you want to do this? It makes no sense.
upvoted 3 times

tom999 3 years, 7 months ago

Agreed. But for the given requirements the answer is right though: D "From the Security settings of the branch, modify the access control for the user. "

upvoted 4 times

aftab7500 3 years, 10 months ago

If you want to bypass branch policies which are already in place. Go to security setting to change them.

upvoted 2 times

Question #13 *Topic 4*

You have an Azure Resource Manager template that deploys a multi-tier application.
You need to prevent the user who performs the deployment from viewing the account credentials and connection strings used by the application.
What should you use?

A. Azure Key Vault

B. a Web.config file

C. an Appsettings.json file

D. an Azure Storage table

E. an Azure Resource Manager parameter file

Suggested Answer: *A*
When you need to pass a secure value (like a password) as a parameter during deployment, you can retrieve the value from an Azure Key Vault. You retrieve the value by referencing the key vault and secret in your parameter file. The value is never exposed because you only reference its key vault ID. The key vault can exist in a different subscription than the resource group you are deploying to.
Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-keyvault-parameter

Community vote distribution
A (100%)

msalvatori Highly Voted 4 years, 2 months ago
Verified - Correct
upvoted 30 times

507101b Most Recent 1 month, 1 week ago
Had this question in my exam today. Option E was not longer an option.
upvoted 1 times

WH16 1 year ago
Selected Answer: A
On exam 2023-09-06, selected A. Azure Key Vault
upvoted 3 times

yana_b 1 year, 1 month ago
Selected Answer: A
Correct answer
upvoted 1 times

catfood 1 year, 1 month ago
Its A with E..... For a static secret, the secret is referenced in a parameter file.
upvoted 2 times

zellck 1 year, 3 months ago
Selected Answer: A
A is the answer.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli
Instead of putting a secure value (like a password) directly in your template or parameter file, you can retrieve the value from an Azure Key Vault during a deployment. You retrieve the value by referencing the key vault and secret in your parameter file. The value is never exposed because you only reference its key vault ID.
upvoted 4 times

surensaluka 1 year, 7 months ago
Selected Answer: A
This question came today (2023-02-14)
upvoted 4 times

syu31svc 2 years, 1 month ago

Selected Answer: A

A for answer

The other options don't make sense at all

upvoted 2 times

Govcomm 2 years, 1 month ago

Azure Key Vault

upvoted 1 times

Mcelona 2 years, 3 months ago

Selected Answer: A

Key Vault

upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: A

correct answer

upvoted 1 times

frutos46 2 years, 10 months ago

Correctly correct

upvoted 3 times

droy89 3 years, 2 months ago

Correct, instead of hard coded creds, AZ key vault instance can be called

upvoted 4 times

RKS 3 years, 7 months ago

Verified - Correct!

upvoted 3 times

samgoomer 3 years, 8 months ago

Is this verified more recently?

upvoted 3 times

d0bermannn 3 years ago

absolutely, if have any disbelief in that , take az104 or az900(not 100% sure about az900)

upvoted 2 times

Rimbik 3 years, 11 months ago

A. Is correct

upvoted 3 times

Question #14 *Topic 4*

SIMULATION -

Your company plans to implement a new compliance strategy that will require all Azure web apps to be backed up every five hours.

You need to back up an Azure web app named az400-123456789-main every five hours to an Azure Storage account in your resource group.

To complete this task, sign in to the Microsoft Azure portal.

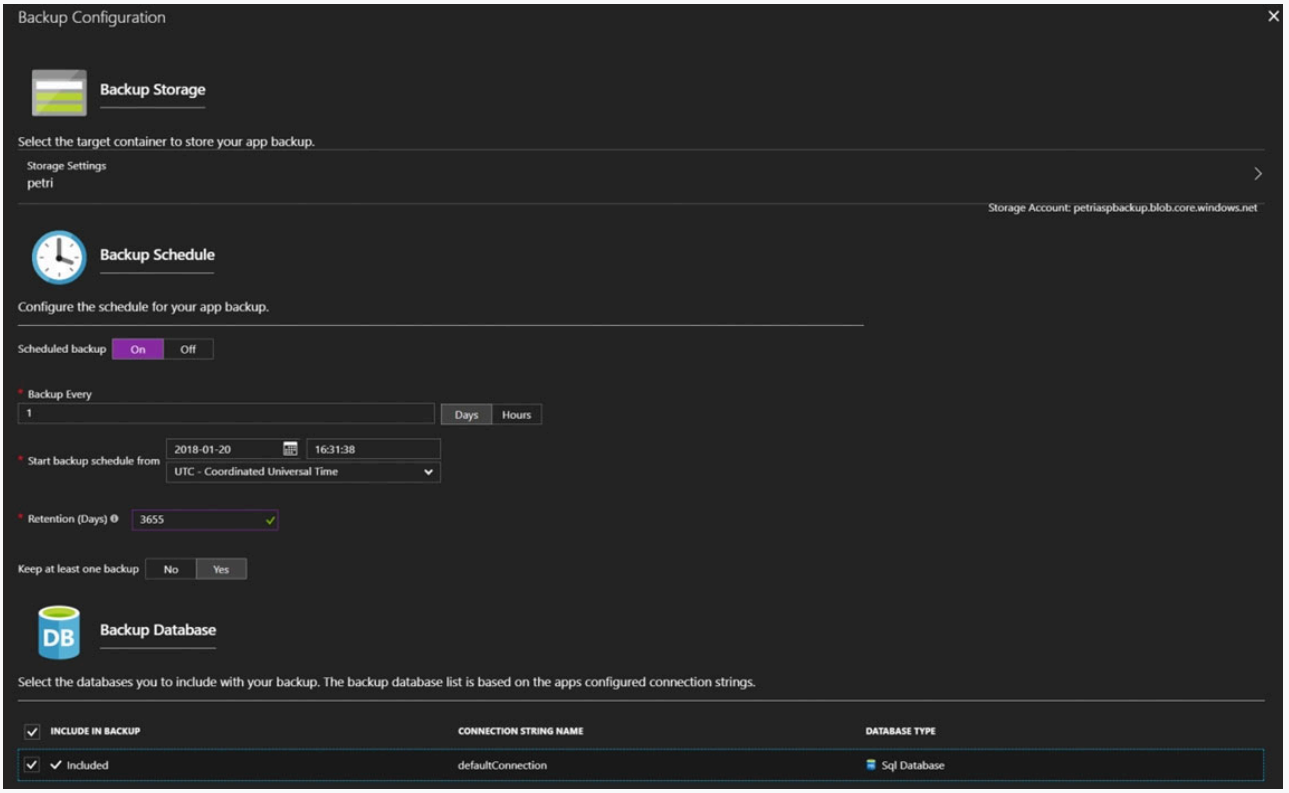
Suggested Answer: *See explanation below.*

With the storage account ready, you can configure backs up in the web app or App Service.

1. Open the App Service az400-123456789-main, which you want to protect, in the Azure Portal and browse to Settings > Backups. Click Configure and a

Backup Configuration blade should appear.

2. Select the storage account.
3. Click + to create a private container. You could name this container after the web app or App Service.
4. Select the container.
5. If you want to schedule backups, then set Scheduled Backup to On and configure a schedule: every five hours
6. Select your retention. Note that 0 means never delete backups.
7. Decide if at least one backup should always be retained.
8. Choose if any connected databases should be included in the web app backup.
9. Click Save to finalize the backup configuration.



Reference:

https://petri.com/backing-azure-app-service

KK787 Highly Voted 3 years, 2 months ago

Are these labs appearing in exam any more?

upvoted 15 times

MBPX 1 year, 4 months ago

Hi not a single lab was in my AZ400 exam this month

upvoted 17 times

Tyler2023 Most Recent 1 year ago

1. Select App Service az400-123456789-main
2. Under Settings -> click Backups
3. Configure custom backups
4. Select the storage account and create new container if there is none

5. Set schedule: Repeats every 5 Hours
6. Click Configure

upvoted 2 times

kingAzure 1 year ago

Is the simulation seperate from the rest of the questions, or can you go back to it after you have answered the other questions?

upvoted 1 times

yana_b 1 year, 1 month ago

Provided guidance is correct, I went under each step.

upvoted 1 times

Govcomm 2 years, 1 month ago

Azure Web App --> Backup

upvoted 2 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 1 times

rdemontis 2 years, 6 months ago

correct answer

upvoted 1 times

Ash111 3 years, 3 months ago

Given answer is correct

Pls ref - https://docs.microsoft.com/en-us/azure/app-service/manage-backup

upvoted 2 times

zioalex 3 years, 3 months ago

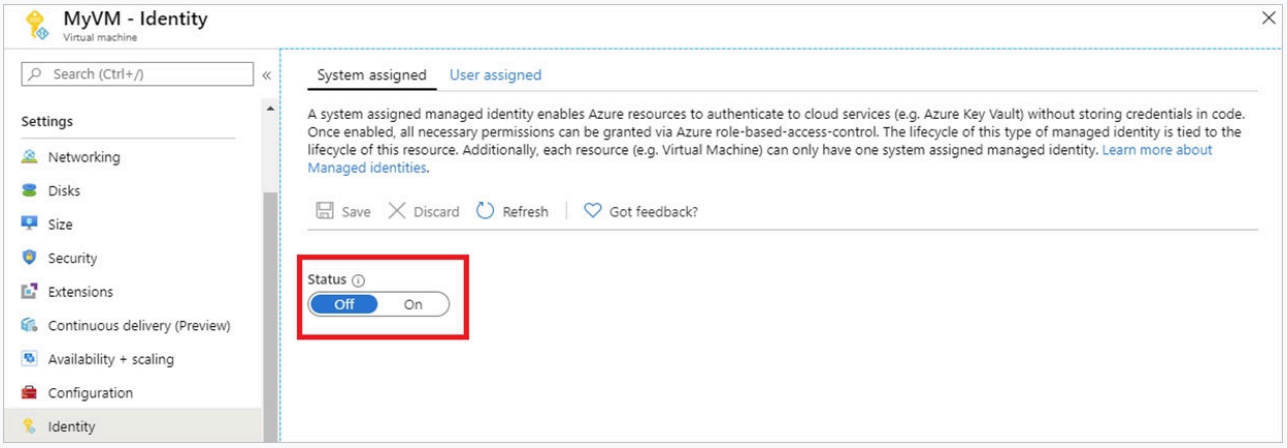
This looks correct to me.

upvoted 2 times

Question #15 *Topic 4*

SIMULATION -
You need to configure a virtual machine named VM1 to securely access stored secrets in an Azure Key Vault named az400-123456789-kv.
To complete this task, sign in to the Microsoft Azure portal.

Suggested Answer: *See explanation below.*
You can use a system-assigned managed identity for a Windows virtual machine (VM) to access Azure Key Vault.
1. Sign in to Azure portal
2. Locate virtual machine VM1.
3. Select Identity
4. Enable the system-assigned identity for VM1 by setting the Status to On.



Note: Enabling a system-assigned managed identity is a one-click experience. You can either enable it during the creation of a VM or in the properties of an existing VM.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-nonaad

stefan1234567 Highly Voted 1 year, 11 months ago
It misses one step to permit the managed identity to access the key vault
upvoted 14 times

Rams_84zO6n Highly Voted 1 year, 6 months ago
Here are the missing steps:
Go to KV - access policy - select permissions - Key - key mgmt- all, key rotation- all, Secret - mgmt- all. After selecting permission, select MI to assign the permission. In this case it is the VM's MI. Look up the MI using the VM MI's object ID. Then click next to make the assignment.
upvoted 10 times

Tyler2023 Most Recent 1 year ago
1. Sign in to Azure portal
2. Locate virtual machine VM1.
3. Select Identity
4. Enable the system-assigned identity for VM1 by setting the Status to On.
5. Allow the managed identity of VM1 in Key vault using Access control (IAM) blade role assignment
upvoted 3 times

renzoku 1 year, 2 months ago
Access Key Vault from Azure virtual machine.
1. Assign Managed Identity to the virtual machine
Enable System-Assigned managed identity for VM1.
This creates an identity for the virtual machine within Azure Active Directory (Azure AD).

2. Configure Key Vault Access Policies
Add Access Policy, select "Virtual Machine VM1"
Add Appropriate permissions, such as "Get" or "List"
Select principal, search and select the "Managed Identity" associated with VM1.

3. Access the Key Vault from VM1

The system-assigned managed identity is enabled for VM1 (OK)

Key Vault access policies are configured (OK)

You can programmatically access the secrets.

upvoted 3 times

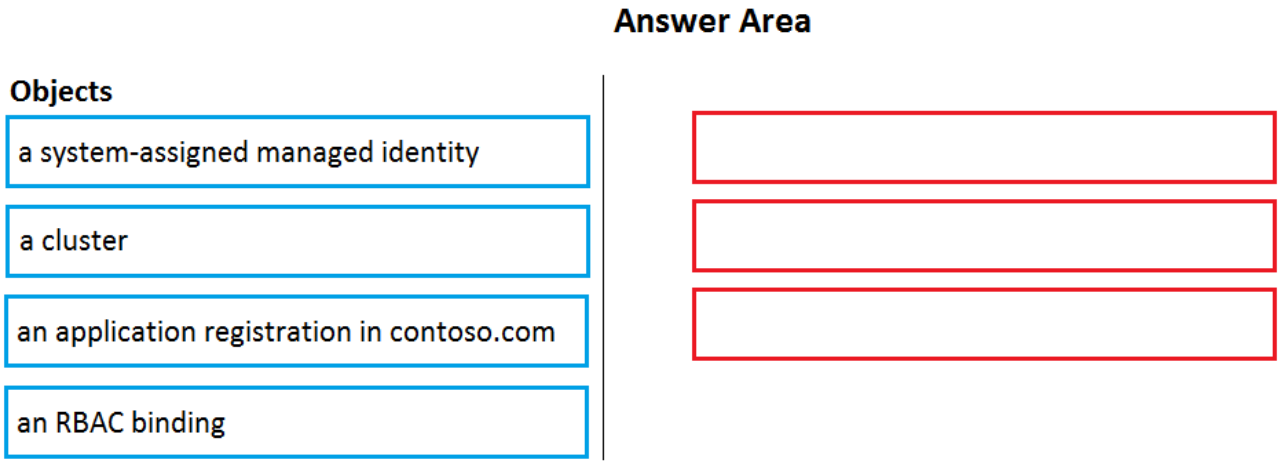
DRAG DROP -

Your company has an Azure subscription named Subscription1. Subscription1 is associated to an Azure Active Directory tenant named contoso.com.

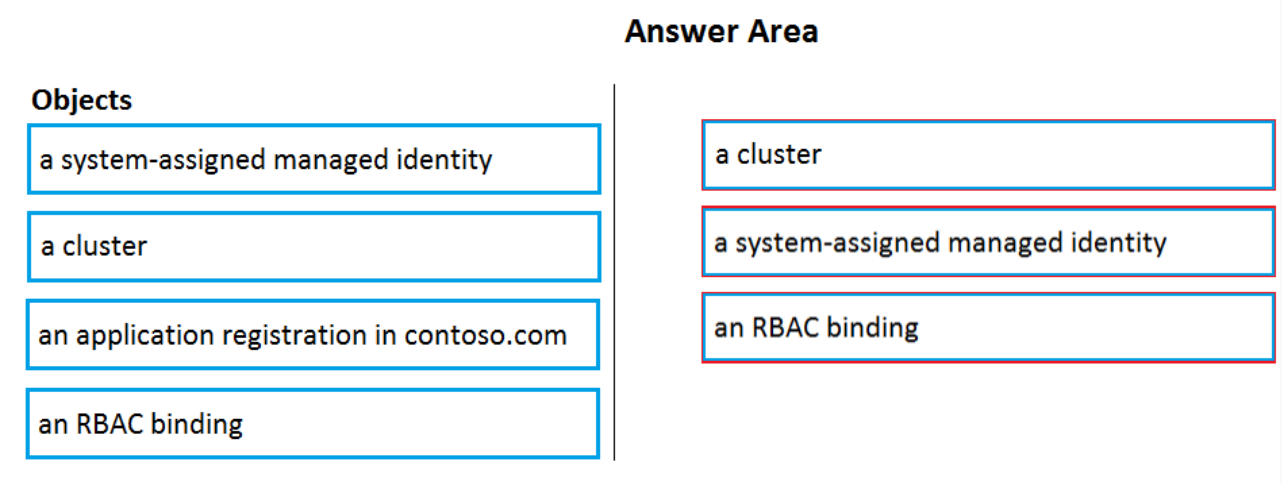
You need to provision an Azure Kubernetes Services (AKS) cluster in Subscription1 and set the permissions for the cluster by using RBAC roles that reference the identities in contoso.com.

Which three objects should you create in sequence? To answer, move the appropriate objects from the list of objects to the answer area and arrange them in the correct order.

Select and Place:



Suggested Answer:

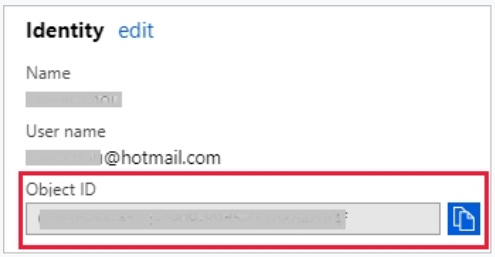


Step 1: Create an AKS cluster -

Step 2: a system-assigned managed identity

To create an RBAC binding, you first need to get the Azure AD Object ID.

1. Sign in to the Azure portal.
2. In the search field at the top of the page, enter Azure Active Directory.
3. Click Enter.
4. In the Manage menu, select Users.
5. In the name field, search for your account.
6. In the Name column, select the link to your account.
7. In the Identity section, copy the Object ID.



Step 3: a RBAC binding -
Reference:
https://docs.microsoft.com/en-us/azure/developer/ansible/aks-configure-rbac

Sylph Highly Voted 3 years, 5 months ago
1. an application registration in contoso.com
2. a cluster
3. an RBAC binding
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli

The new, improved way: https://docs.microsoft.com/en-us/azure/aks/managed-aad
upvoted 61 times

LeeVee 3 years, 5 months ago
This is correct.
upvoted 2 times

yaziciali 3 years, 5 months ago
it makes more sense
upvoted 2 times

Beast_Hollow 3 years, 4 months ago
Why, when you are creating the AKS cluster in the subscription that is tied to contoso.com?
upvoted 2 times

rdemontis 2 years, 6 months ago
I think you are correct. The requirement is to allow AAD users from the contoso.com tenant to access the cluster. But to do this what do you need a system assigned managed identity for?
These identities are automatically generated by the azure service and are used to allow the service itself to access other azure resources or any other service that supports AAD authentication.

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview#how-can-i-use-managed-identities-for-azure-resources

You can find the solution (even if now it is a legacy solution) to allow AAD users to access the cluster in the following document:

https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli
upvoted 3 times

rdemontis 2 years, 6 months ago
As we can see we need to create two app registrations, one for the Server and one for the Client component, on AAD before creating the cluster. The same thing is stated in the link provided in the examtopics explanation.

https://docs.microsoft.com/en-us/azure/developer/ansible/aks-configure-rbac

Just look at the section "Configure Azure AD for AKS authentication" and the yaml file used to create the cluster (section "aad_profile").

Clearly, you need to create the app registrations first. I think the answers proposed in the question are not precise because they specify the need for only one app registration. But since system-assigned managed identity doesn't make any sense in this context the correct answer is:

1. an application registration in contoso.com
2. a cluster
3. an RBAC binding
upvoted 6 times

JohnWix Highly Voted 3 years, 5 months ago
I think the answer provided is correct. You dont need to register application in Contoso.com
upvoted 38 times

noussa 3 years, 4 months ago

That's my opinion too
upvoted 4 times

HetalMehta24 Most Recent 3 months ago
This is correct.
upvoted 2 times

vsvaid 9 months ago
Agree with suggested answer
--Create Cluster
--Create Managed identity
--Assigned required RBAC
upvoted 3 times

KumaTed 1 year, 2 months ago
when use system-assigned managed identity, should be only two steps
1. a cluster
2. an RBAC binding

Managed identities are the recommended way to authenticate with other resources in Azure, and is the default authentication method for your AKS cluster.
https://learn.microsoft.com/en-us/azure/aks/kubernetes-service-principal?tabs=azure-cli

A system-assigned managed identity is automatically created when you create an AKS cluster.
https://learn.microsoft.com/en-us/azure/aks/use-managed-identity
---
when use service principle, should be three steps
1. a cluster
2. an application registration in contoso.com
3. an RBAC binding
https://learn.microsoft.com/en-us/azure/aks/kubernetes-service-principal?tabs=azure-cli
upvoted 4 times

Takj81 10 months, 2 weeks ago
This is correct.
upvoted 2 times

Cervezerg 1 year, 3 months ago
ChatGPT answer:
1) an application registration in contoso.com: First, you need to create an application registration (also known as a service principal) in the Azure Active Directory tenant contoso.com. This application registration represents the identity that will be used to authenticate and authorize access to the AKS cluster.

2) a cluster: Once you have the application registration in place, you can provision the AKS cluster in Subscription1. During the creation process, you will associate the cluster with the contoso.com Azure Active Directory tenant.

3) an RBAC binding: After the AKS cluster is provisioned, you need to set the permissions and access controls for the cluster using RBAC (Role-Based Access Control). RBAC allows you to define roles and assign them to specific users, groups, or service principals. In this step, you will create an RBAC binding that references the identities in contoso.com and grant them the appropriate roles and permissions for the AKS cluster.
upvoted 4 times

randomaccount123 1 year, 5 months ago
It is now recommended to use Managed Identities over Service Principals for AKS Clusters. Therefore the answer is correct.
upvoted 2 times

mohiniu 1 year, 6 months ago
https://www.youtube.com/watch?v=mulBa_No4hw&t=1s
Explain RBAC on AKS
upvoted 1 times

syu31svc 2 years, 1 month ago
Given answer is correct and supported by provided link
upvoted 3 times

Mcelona 2 years, 3 months ago
In my opinion the answer is correct.
upvoted 3 times

darsh19 2 years, 8 months ago
1- AKS cluster
2- System assigned managed identity
3- RBAC binding
upvoted 9 times

frutos46 2 years, 10 months ago
Its correct
upvoted 2 times

ukkuru 3 years, 1 month ago
Please look at the options in AKS cluser creation page
Basics
Node pools
Authentication
Networking
Integrations
Tags
Review + create
Cluster infrastructure
The cluster infrastructure authentication specified is used by Azure Kubernetes Service to manage cloud resources attached to the cluster. This can be either a service principal or a system-assigned managed identity.
Authentication method
Service principal
System-assigned managed identity

Kubernetes authentication and authorization
Authentication and authorization are used by the Kubernetes cluster to control user access to the cluster as well as what the user may do once authenticated.Learn more about Kubernetes authentication
Role-based access control (RBAC)
Enabled
Disabled

AKS-managed Azure Active Directory
Node pool OS disk encryption
By default, all disks in AKS are encrypted at rest with Microsoft-managed keys. For additional control over encryption, you can supply your own keys using a disk encryption set backed by an Azure Key Vault. The disk encryption set will be used to encrypt the OS disks for all node pools in the cluster.Learn more
upvoted 1 times

MaTaO 3 years, 2 months ago
I think provided answer is correct
when you create AKS in the portal,
in Authentication tab you either select
System assigned managed identity or Service principal (this step you need to create an app in AAD first) then set up RBAC below
upvoted 3 times

amanp 3 years, 2 months ago
App registrations is not required when setting up AKS. The given answer is correct
upvoted 3 times

Question #17 *Topic 4*

HOTSPOT -

You manage build and release pipelines by using Azure DevOps. Your entire managed environment resides in Azure.

You need to configure a service endpoint for accessing Azure Key Vault secrets. The solution must meet the following requirements:

➪ Ensure that the secrets are retrieved by Azure DevOps.

➪ Avoid persisting credentials and tokens in Azure DevOps.

How should you configure the service endpoint? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Service connection type:
- Azure Resource Manager
- Generic service
- Team Foundation Server / Azure Pipelines service connection

Authentication/authorization method for the connection:
- Azure Active Directory OAuth 2.0
- Grant authorization
- Managed Service Identity Authentication

Suggested Answer:

Answer Area

Service connection type:
- Azure Resource Manager
- Generic service
- Team Foundation Server / Azure Pipelines service connection

Authentication/authorization method for the connection:
- Azure Active Directory OAuth 2.0
- Grant authorization
- Managed Service Identity Authentication

Box 1: Azure Pipelines service connection

Box 2: Managed Service Identity Authentication

The managed identities for Azure resources feature in Azure Active Directory (Azure AD) provides Azure services with an automatically managed identity in Azure

AD. You can use the identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without any credentials in your code.

Reference:

https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/deploy/azure-key-vault https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

jhxetc Highly Voted 3 years ago

https://azuredevopslabs.com/labs/vstsextend/azurekeyvault/

Task 3 Step 6 - The answer for part 1 should definitely be ARM

upvoted 36 times

Lyonel Highly Voted 3 years, 1 month ago

Here is what the link (link: https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/deploy/azure-key-vault?view=azure-devops] provided states under 'Prerequisites':

"An Azure subscription linked to Azure Pipelines or Team Foundation Server using the Azure Resource Manager service connection."

Answer #1 is CORRECT (Team Foundation Server / Azure Pipelines service connection). It appears that the answer is worded wrongly or even

poorly, but is CORRECT.

As for Answer #2, specified in the second link provided [link: https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview]: "Managed identities eliminate the need for developers to manage credentials."

So, as specified in the question -- "Avoid persisting credentials and tokens in Azure DevOps." Answer #2 is CORRECT (Managed Service Identity Authentication), as it states in the link, "Managed identities eliminate the need for developers to manage credentials."
upvoted 24 times

djhyfdgjk 7 months, 1 week ago
And how are you going to assign Managed Identity to Azure Devops organization ?? As far as I know it is not possible. Therefore correct answers should be ARM Service Connection and Authorization.
upvoted 1 times

mmdex 1 year, 8 months ago
Answer #1 should be "Azure Resource Manager". It isn't worded wrongly. The "Team Foundation Server / Azure Pipelines service connection" type simply does not exist. The "Azure Resource Manager" and "Generic" service connection types do exist. Here is a list of common service connection types:
https://learn.microsoft.com/en-us/azure/devops/pipelines/library/service-endpoints?view=azure-devops&tabs=yaml#common-service-connection-types
upvoted 5 times

rdemontis 2 years, 6 months ago
No it isn't worded wrongly. "An Azure subscription linked to Azure Pipelines or Team Foundation Server using the Azure Resource Manager service connection" means you have already an ARM service connection in the devops project or in the pipeline that links to your Azure subscription. You need it to access to any azure resource in your azure subscription. So the provided answer #1 is wrong. ARM is correct
upvoted 14 times

Christian_garcia_martin Most Recent 3 weeks, 2 days ago
Copilot : Service connection type: Azure Resource Manager
Authentication/authorization method for the connection: Managed Service Identity Authentication
upvoted 1 times

FeriAZ 6 months, 1 week ago
Service connection type: Azure Resource Manager
Authentication/authorization method for the connection: Managed Service Identity (MSI)

Azure Resource Manager service type: This service connection type specifically targets Azure resources, including Key Vault. It allows your pipeline to interact with Key Vault using the Managed Service Identity assigned to the Azure DevOps project.
Managed Service Identity (MSI) authentication: This eliminates the need to store sensitive information like credentials or tokens within your pipeline. Instead, the pipeline leverages its assigned MSI to access resources securely. Azure automatically manages and rotates the MSI credentials, enhancing security and reducing the risk of exposure.
upvoted 2 times

ozbonny 6 months, 3 weeks ago
ARM and Manage Identity
upvoted 1 times

codeByJazz 7 months ago
copilot says : GitHub Copilot
To configure a service endpoint for accessing Azure Key Vault secrets without persisting credentials and tokens in Azure DevOps, you should use Managed Service Identity (MSI).

Here are the steps:

Enable Managed Service Identity (MSI) on your Azure DevOps. This will create an identity for your Azure DevOps in Azure Active Directory.

Assign the necessary permissions to the MSI in Azure Key Vault. You can do this by adding an access policy in Key Vault that gives the MSI the necessary permissions (like Get, List) to retrieve secrets.

In Azure DevOps, when creating the service connection for Azure Key Vault, choose "Managed identity" as the Authentication method.

This way, Azure DevOps will use the managed identity to authenticate to Azure Key Vault and retrieve secrets, and you won't need to store any credentials or tokens in Azure DevOps.
upvoted 1 times

vsvaid 9 months ago
ARM and Managed Service
upvoted 1 times

varinder82 9 months, 3 weeks ago
Final Answer After all comments analysis:
1. Azure Resource Manager
2. Managed Service Identity Authentication
upvoted 5 times

Spectrum128k 10 months, 3 weeks ago
Can we discourage people posting answers from ChatGPT? I can use that myself and it's often wrong on the simplest things!
upvoted 13 times

yana_b 1 year, 1 month ago
Following the URLs provided by Lyonel, it seems that provided answer is correct
upvoted 1 times

318touring 1 year, 4 months ago
According to ChatGPT, and the usual way of doing things:

"
To configure a service endpoint for accessing Azure Key Vault secrets while meeting the given requirements, you should use the Azure Resource Manager service endpoint type.

Here are the steps to configure the service endpoint:

In Azure DevOps, navigate to the project where you want to create the service endpoint.
Go to Project Settings and select Service connections under Pipelines.
Click on New service connection and select Azure Resource Manager."
upvoted 1 times

Rams_84zO6n 1 year, 6 months ago
AzureResourceManager, Managed Service Identity Authentication
Step1: Enabled KV for ARM deployment
Ste[2: To the devops project, add a ARM service connection and select ARM Service Identity for authentication, provide your cloud subscription, tenant id, provide a name for service connection, grant permission to all pipelines, save.
upvoted 3 times

mohiniu 1 year, 6 months ago
Azure Pipelines supports the following service connection types by default. Any service connection other than ARM doesnt look relevant.

Azure Classic | Azure Repos/TFS | Azure Resource Manager | Azure Service Bus | Bitbucket | Chef | Docker hub or others | Other Git | Generic | GitHub | GitHub Enterprise Server | Jenkins | Kubernetes | Maven | npm | NuGet | Python package download | Python package upload | Service Fabric | SSH | Subversion | Visual Studio App Center |
upvoted 1 times

mohiniu 1 year, 6 months ago
Also in reference link of answer its mentioned:
An Azure subscription linked to Azure Pipelines or Team Foundation Server using the Azure Resource Manager service connection. So answer should be ARM
upvoted 1 times

reks2022 1 year, 9 months ago
azureresourcemanager & managed identity
upvoted 2 times

syu31svc 2 years, 1 month ago

https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/deploy/azure-key-vault?view=azure-devops

"An Azure subscription linked to Azure Pipelines or Team Foundation Server using the Azure Resource Manager service connection."

Service connection is ARM

"Avoid persisting credentials and tokens" so this would be managed identity for authentication
upvoted 1 times

Eltooth 2 years, 4 months ago
ARM and MI are correct.
upvoted 2 times

UnknowMan 2 years, 4 months ago
Arm + Managed identity (to not store, access token etc..)
upvoted 5 times

Question #18 *Topic 4*

You are deploying a server application that will run on a Server Core installation of Windows Server 2019.
You create an Azure key vault and a secret.
You need to use the key vault to secure API secrets for third-party integrations.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Configure RBAC for the key vault.

B. Modify the application to access the key vault.

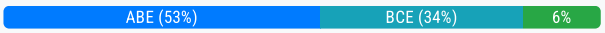
C. Configure a Key Vault access policy.

D. Deploy an Azure Desired State Configuration (DSC) extension.

E. Deploy a virtual machine that uses a system-assigned managed identity.

Suggested Answer: *BCE*
BE: An app deployed to Azure can take advantage of Managed identities for Azure resources, which allows the app to authenticate with Azure Key Vault using
Azure AD authentication without credentials (Application ID and Password/Client Secret) stored in the app.
C:
1. Select Add Access Policy.
2. Open Secret permissions and provide the app with Get and List permissions.
3. Select Select principal and select the registered app by name. Select the Select button.
4. Select OK.
5. Select Save.
6. Deploy the app.
Reference:
https://docs.microsoft.com/en-us/aspnet/core/security/key-vault-configuration

Community vote distribution



Marang73 Highly Voted 3 years, 10 months ago
B, C, E is possible see https://docs.microsoft.com/en-us/azure/key-vault/general/tutorial-net-virtual-machine

RBAC is also possible but it still in preview https://docs.microsoft.com/en-us/azure/key-vault/general/rbac-guide
upvoted 30 times

Tyler2023 1 year ago
RBAC is the recommended authorization now, I understand Marang73 comments was almost 3 years ago, but for others going to see this, use RBAC if possible
upvoted 9 times

catfood 1 year, 2 months ago
not in preview any more, so could be either access policy or RBAC. When creating a key vault, "Azure role-based access control (recommended)" is shown in the portal.
upvoted 8 times

kumardeb Highly Voted 3 years, 10 months ago
B. Modify the application to access the key vault.
C. Configure a Key Vault access policy.
E. Deploy a virtual machine that uses a system-assigned managed identity.
upvoted 7 times

only_juans Most Recent 1 week ago
Selected Answer: ABE
As of today, ABE is the best choice.
upvoted 1 times

hajurbau 3 months ago

Selected Answer: ABE

ABE and BCW are both acceptable solutions. However, I am now going with ABE as RBAC as the new recommended authorisation.

upvoted 2 times

ay_m 3 months, 1 week ago

Selected Answer: ABE

RBAC is now the recommended method for key vault, and access policies are considered legacy by Microsoft. This link further clarifies this change.

https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-access-policy

upvoted 2 times

UrbanRellik 4 months ago

Selected Answer: ABE

1) E, deploy a VM that uses a system-assigned managed identity.
2) A, configure RBAC for the Key Vault and assign the system managed identity access.
3) B, modify the application to access the key vault as desired.

upvoted 1 times

ozbonny 6 months, 3 weeks ago

Selected Answer: BDE

I think BCE

upvoted 2 times

cluqueg 10 months, 1 week ago

Selected Answer: ABE

Now it's recommended to use RBAC instead.

upvoted 5 times

Tyler2023 1 year ago

RBAC is now recommended authz, if I'm going to do this in sequence, I will do E,A,B

upvoted 4 times

ieboaix 1 year, 1 month ago

B, C and E are correct the answer. B and C are obvious. while A is possible when the app is registered with AAD. but here it hints the app is deployed in a VM with a managed identity, hence, E is chosen.

upvoted 2 times

flafernan 1 year, 1 month ago

A,B,C - Option E is not required to ensure secure access to Key Vault secrets by the application running on the server. Using a system-assigned managed identity (system-assigned managed identity) is useful when you want the virtual machine itself to have an identity to access resources such as Key Vault directly. However, in this specific scenario, the objective is to modify the application to access the Key Vault, and this is done by configuring the accepted permissions (RBAC) and a Key Vault access policy, which does not require the use of an identity managed by the Key Vault. virtual machine. Therefore, option E is not needed in this situation and can be excluded from the choices. Options A, B and C are the most suitable to meet the specific requirements of the presented scenario.

upvoted 4 times

xRiot007 1 year, 2 months ago

E,C,B
E - you need to assign a managed identity to your VM
C - you create a policy for that managed identity to give it permissions
B - you have to modify your app to retrieve values from the KV before usage. It will use DefaultAzureCredential

upvoted 2 times

xRiot007 1 year, 2 months ago

https://learn.microsoft.com/en-us/azure/key-vault/general/tutorial-net-virtual-machine?tabs=azure-cli

upvoted 1 times

Pamban 1 year, 3 months ago

Selected Answer: BCE

Definitely B,C and E

I have engaged these sort of activities many times in greenfield deployments

upvoted 1 times

diego84 1 year, 9 months ago

Selected Answer: ABE

E - it is for VM

A- Set up MI over KV using RBAC

B - Change your app to use the MI

upvoted 6 times

meoukg 1 year, 10 months ago

BCE were my chosen answers yesterday when I sat on this exam

upvoted 2 times

Def21 2 years ago

BE are quite clear. It is either ABE or BCE.

If you have system-assigned managed identity, you should be able to use RBAC for it. This is, to my understanding, preferred solution. So ABE.

However, in the links provided, the instructions always talk about access policies. Not sure if they are just legacy. Thus, BCE. At least this should work.

upvoted 3 times

syu31svc 2 years, 1 month ago

Selected Answer: BCE

https://docs.microsoft.com/en-us/azure/key-vault/general/tutorial-net-virtual-machine?tabs=azure-cli

https://docs.microsoft.com/en-us/aspnet/core/security/key-vault-configuration?view=aspnetcore-6.0

BCE are correct

upvoted 1 times

Question #19 *Topic 4*

HOTSPOT -

Your company is creating a suite of three mobile applications.

You need to control access to the application builds. The solution must be managed at the organization level.

What should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Groups to control the build access:

- Active Directory groups
- Azure Active Directory groups
- Microsoft Visual Studio App Center distribution groups

Group type:

- Private
- Public
- Shared

Suggested Answer:

Answer Area

Groups to control the build access:

- Active Directory groups
- Azure Active Directory groups
- Microsoft Visual Studio App Center distribution groups

Group type:

- Private
- Public
- Shared

Box 1: Microsoft Visual Studio App Center distribution Groups

Distribution Groups are used to control access to releases. A Distribution Group represents a set of users that can be managed jointly and can have common access to releases. Example of Distribution Groups can be teams of users, like the QA Team or External Beta Testers or can represent stages or rings of releases, such as Staging.

Box 2: Shared -

Shared distribution groups are private or public distribution groups that are shared across multiple apps in a single organization. Shared distribution groups eliminate the need to replicate distribution groups across multiple apps.

Note: With the Deploy with App Center Task in Visual Studio Team Services, you can deploy your apps from Azure DevOps (formerly known as VSTS) to App

Center. By deploying to App Center, you will be able to distribute your builds to your users.

Reference:

https://docs.microsoft.com/en-us/appcenter/distribution/groups

AS007 Highly Voted 4 years, 4 months ago

Correct Answer - verified

upvoted 40 times

binq Highly Voted 2 years, 7 months ago

Correct. Private, Public, and Shared are groups available only in App Center. Shared is a Private or Public group that is shared between multiple apps (here 3).

upvoted 7 times

Fal991l Most Recent 1 year, 5 months ago

GPT:Microsoft Visual Studio App Center Distribution groups should be used to control access to the application builds, and the group type should be set to Private. Private distribution groups are accessible only to the testers who are invited via email, which ensures that only authorized users have access to the builds. Shared distribution groups, on the other hand, can be accessed by multiple apps in the organization, which may not be desirable if the builds are intended only for specific groups or stages. Therefore, the correct answer is:

Groups to control the build access: Microsoft Visual Studio App Center Distribution groups
Group Type: Private
upvoted 1 times

syu31svc 2 years, 1 month ago
Answer is correct and explanation given supports it
upvoted 1 times

Govcomm 2 years, 1 month ago
Mobile Applications --> Visual Studio App Center --> Shared for all applications
upvoted 1 times

UnknowMan 2 years, 4 months ago
Correct,

This groups is only available on appcenter and we need Shared group because we have 3 apps
upvoted 2 times

rdemontis 2 years, 5 months ago
correct answer
upvoted 2 times

ScreamingHand 3 years, 2 months ago
Well done Exam Topics - correct answer!
upvoted 3 times

RKS 3 years, 7 months ago
Verified - Correct!
upvoted 2 times

sugarbubbles 3 years, 10 months ago
repeated on topic 14 question 7
upvoted 3 times

Question #20 *Topic 4*

You have an Azure DevOps organization named Contoso that contains a project named Project1.
You provision an Azure key vault named Keyvault1.
You need to reference Keyvault1 secrets in a build pipeline of Project1.
What should you do first?

A. Add a secure file to Project1.

B. Create an XAML build service.

C. Create a variable group in Project1.

D. Configure the security policy of Contoso.

Suggested Answer: *D*
Before this will work, the build needs permission to access the Azure Key Vault. This can be added in the Azure Portal.
Open the Access Policies in the Key Vault and add a new one. Choose the principle used in the DevOps build.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/release/azure-key-vault

Community vote distribution
C (100%)

Hooters Highly Voted 3 years, 10 months ago
C. Create a variable group in Project1.
upvoted 77 times

Tyler2023 1 year ago
Agree, you need to create a variable group in Project1 -> Pipelines -> Library -> Click + Variable group -> Enable the "Link secrets from an Azure key vault as variables"
upvoted 2 times

yhredil Highly Voted 3 years, 10 months ago
C - is the right one
https://docs.microsoft.com/en-us/azure/devops/pipelines/library/variable-groups?view=azure-devops&tabs=yaml#link-secrets-from-an-azure-key-vault
upvoted 12 times

GPRai Most Recent 2 months, 3 weeks ago
C. Create a variable group in Project1.
upvoted 1 times

de89f6b 3 months, 4 weeks ago
Selected Answer: C
C. Create a variable group
upvoted 1 times

FeriAZ 6 months, 1 week ago
Variable groups are specifically designed to store and manage sensitive information like Key Vault secrets within Azure DevOps. They offer several advantages:
Centralized management: You can store and manage all your secrets in one place, making them easy to access and update across different pipelines within the project.
Security: Variable groups offer security features like access control, which allows you to control who can access and modify the stored secrets.
Integration with pipelines: You can easily reference secrets stored in variable groups within your build pipelines using dedicated tasks.
upvoted 1 times

ozbonny 6 months, 3 weeks ago
in the question says you provision an azure key vault and it means all needed configurations were applied to it.

so according with this lab the most accurate answer is C. Create a variable group in Project1

https://microsoftlearning.github.io/AZ400-DesigningandImplementingMicrosoftDevOpsSolutions/Instructions/Labs/AZ400_M05_L10_Integrating_Azure_Key_Vault_with_Azure_DevOps.html

upvoted 1 times

vsvaid 9 months ago

Selected Answer: C

Agree with selected answer

upvoted 1 times

renzoku 1 year, 2 months ago

Selected Answer: C

C. Create a variable group in Project1.

To reference Keyvault1 secrets in a build pipeline, you need to create a variablegroup.

Azure DevOps variable groups can link to Azure Key Vault.

upvoted 1 times

318touring 1 year, 4 months ago

Selected Answer: C

As others have said, link secrets from KV

upvoted 1 times

mohiniu 1 year, 6 months ago

Selected Answer: C

Create a variable group in Project1 . Creating variable group is current. We need no do change anything at organisation contoso level

upvoted 1 times

surensaluka 1 year, 8 months ago

Selected Answer: C

https://www.examtopics.com/exams/microsoft/az-400/view/12/

Q23 also says the variable group is the answer.

upvoted 1 times

bellorg 1 year, 8 months ago

C. Create a variable group in Project1

upvoted 1 times

Rachid 1 year, 9 months ago

C

I just check : Security policies ib organization settings cannot solve KV access.

upvoted 2 times

Rachid 1 year, 9 months ago

D

It Says wht you do FIRST

without givind access to List KV secret to SP of Devops , you wont be able to read an set a variable

upvoted 1 times

joshfry 1 year, 8 months ago

As Contoso is the Azure DevOps instance, and not the Key Vault.

upvoted 1 times

meoukg 1 year, 10 months ago

I chose C when I sat on this exam, and I passed :)

upvoted 2 times

DParekh 1 year, 12 months ago

C is correct answer. Why D is not correct? To access AKV from build pipeline, we have to define access policy at Azure Key Vault level. D is saying configure security policy of Contoso project which is not correct.

upvoted 2 times

syu31svc 2 years, 1 month ago

Selected Answer: C

Answer is C

https://docs.microsoft.com/en-us/azure/devops/pipelines/library/variable-groups?view=azure-devops&tabs=yaml

"Variable groups store values and secrets that you might want to be passed into a YAML pipeline or make available across multiple pipelines. You can share and use variable groups in multiple pipelines in the same project."

"Link an existing Azure key vault to a variable group and map selective vault secrets to the variable group."

upvoted 1 times

Question #22 *Topic 4*

You have the following Azure policy.

```
if: {
   allof: [
       {
              "field": "type",
              "equals": "Microsoft.Storage/storageAccounts"
       },
       {
              "field": "Microsoft.Storage/storageAccounts/supportsHttpsTrafficOnly",
              "notEquals": "true"
       }
   ]
},
then: {
   effect: "deny"
}
```

You assign the policy to the Tenant root group.
What is the effect of the policy?

A. prevents all HTTP traffic to existing Azure Storage accounts

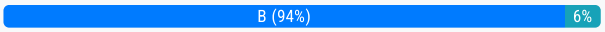
B. ensures that all traffic to new Azure Storage accounts is encrypted

C. prevents HTTPS traffic to new Azure Storage accounts when the accounts are accessed over the Internet

D. ensures that all data for new Azure Storage accounts is encrypted at rest

Suggested Answer: *B*
Denies non HTTPS traffic.

Community vote distribution



rafapaz09 Highly Voted 3 years, 4 months ago
Correct answer is good, the policy is not going to apply to the existing resources, unless you run a remediation task to force the policy to all the existing resources
upvoted 25 times

Kinon4 Highly Voted 3 years, 4 months ago
If storage accounts don't support HTTPS only, then deny. Therefore answer is A, only accepts encrypted traffic.
upvoted 14 times

Kinon4 3 years, 4 months ago
Answer is B**
upvoted 12 times

CyberLumi 3 years, 3 months ago
The policy denies the creation of any new storage account that does not allow the https protocol. It is a DENY policy not a policy to allow https traffic. Answer is B
upvoted 15 times

hajurbau Most Recent 2 months, 1 week ago
Answer A is also correct if the remediation is ran. But selecting B for now
upvoted 1 times

ozbonny 6 months, 3 weeks ago
Selected Answer: B
B. ensures that all traffic to new Azure Storage accounts is encrypted
upvoted 3 times

GokhanSenyuz 1 year, 10 months ago

Selected Answer: B

answer B

That's the cheese!

upvoted 1 times

Atos 2 years ago

The code just seems unnecessary and answers just as bad. From what i understand it has 2 negative clauses that would effectively mean the https rule is enforced, so the storage traffic is securely encrypted.

Ans: B.

upvoted 3 times

syu31svc 2 years, 1 month ago

Selected Answer: B

Not equals true then deny is the key here

You do not allow traffic if it is not HTTPS

Answer is B

upvoted 1 times

Govcomm 2 years, 1 month ago

All traffic to the Azure Storage Account is encrypted through HTTPS

upvoted 1 times

Eltooth 2 years, 4 months ago

Selected Answer: B

B is correct answer.

upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct and you can run "remediation task for existing resources.

upvoted 1 times

Cheehp 2 years, 5 months ago

Selected during exam.

B. ensures that all traffic to new Azure Storage accounts is encrypted

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: B

This is the reason why the correct answer is B: "During evaluation of existing resources, resources that match a deny policy definition are marked as non-compliant"

https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects#deny

upvoted 2 times

sujitwarrier11 2 years, 7 months ago

Selected Answer: B

Correct answer B. Azure policy wont affect existing resources I think, only the newly created once after policy is enforced are affected.

upvoted 1 times

binq 2 years, 7 months ago

Selected Answer: B

Correct. Policy denies all future storage accounts that don't support HTTPS. Policies don't affect existing resources, hence A is incorrect.

upvoted 3 times

PlumpyTumbler 2 years, 7 months ago

Selected Answer: B

Word up. It's B, I'm not going to put the same link everyone else provided. This is a well documented answer.

upvoted 1 times

Shreyans 2 years, 7 months ago

Selected Answer: B

Correct Answer is B

upvoted 2 times

Sst121 2 years, 8 months ago

Selected Answer: A

Ans: A

upvoted 1 times

Question #23 *Topic 4*

You have an Azure DevOps organization named Contoso, an Azure DevOps project named Project1, an Azure subscription named Sub1, and an Azure key vault named vault1.
You need to ensure that you can reference the values of the secrets stored in vault1 in all the pipelines of Project1. The solution must prevent the values from being stored in the pipelines.
What should you do?

A. Create a variable group in Project1.

B. Add a secure file to Project1.

C. Modify the security settings of the pipelines.

D. Configure the security policy of Contoso.

Suggested Answer: *A*
Use a variable group to store values that you want to control and make available across multiple pipelines.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/library/variable-groups

Community vote distribution
A (100%)

AS007 Highly Voted 4 years, 4 months ago
Correct
upvoted 25 times

thijsvb Highly Voted 3 years, 11 months ago
Anwer is correct, because in a variable group you can link a key vault. Then you can make the group available to everyone. This way you can ensure that every pipeline can use the variables. Better useability then using tasks in every pipeline.
upvoted 13 times

gautamksr 3 years, 9 months ago
correct
upvoted 2 times

GPRai Most Recent 2 months, 3 weeks ago
Selected Answer: A
Correct
upvoted 1 times

ozbonny 6 months, 3 weeks ago
Selected Answer: A
A. Create a variable group in Project1.
upvoted 1 times

vsvaid 9 months ago
Selected Answer: A
Agree with A
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: A
Correct answer and relevant explanation
upvoted 1 times

Mcelona 1 year, 8 months ago
Selected Answer: A
A is the correct answer
upvoted 1 times

meoukg 1 year, 10 months ago
I chose A when I sat on this exam, and I passed :)

upvoted 2 times

syu31svc 2 years, 1 month ago

Selected Answer: A

Given link supports A as the answer

upvoted 1 times

Govcomm 2 years, 1 month ago

Variable group for accessing Azure Key Vault

upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: A

Correct answer
https://docs.microsoft.com/en-us/azure/devops/pipelines/library/variable-groups?view=azure-devops&tabs=yaml#link-secrets-from-an-azure-key-vault

upvoted 3 times

celciuz 3 years ago

This question came out too, August 2021

upvoted 3 times

francis6170 3 years, 2 months ago

Got this in the AZ-400 exam (June 2021).

upvoted 3 times

Kalaismile06 3 years, 3 months ago

Question already repeated.

upvoted 1 times

MacawLord 3 years, 1 month ago

It's quite similar to Question #23 in this same question set, only differences are this one has an Azure subscription and needs to prevent the values from being stored in pipelines

upvoted 2 times

Yogothegreat 4 years, 4 months ago

Using Variable Group is a right answer but
Secrets stored in vault1 in all the pipelines of Project1 can be directly accessed if we add a KeyVault Task in the pipeline, whats the purpose of reading it into Variable group, for sharing it across many stages in pipeline ? can someone throw more light

upvoted 6 times

hart232 4 years, 4 months ago

Looks to be a near appropriate answer compared to the available options.

upvoted 1 times

Doenoe 4 years, 3 months ago

I think it's the better choice from a security perspective. You would populate the variable group from KeyVault periodically and only when needed, instead of querying the 'external' KeyVault for secrets everytime the pipeline runs.

upvoted 6 times

DRAG DROP -

You use GitHub Enterprise Server as a source code repository.

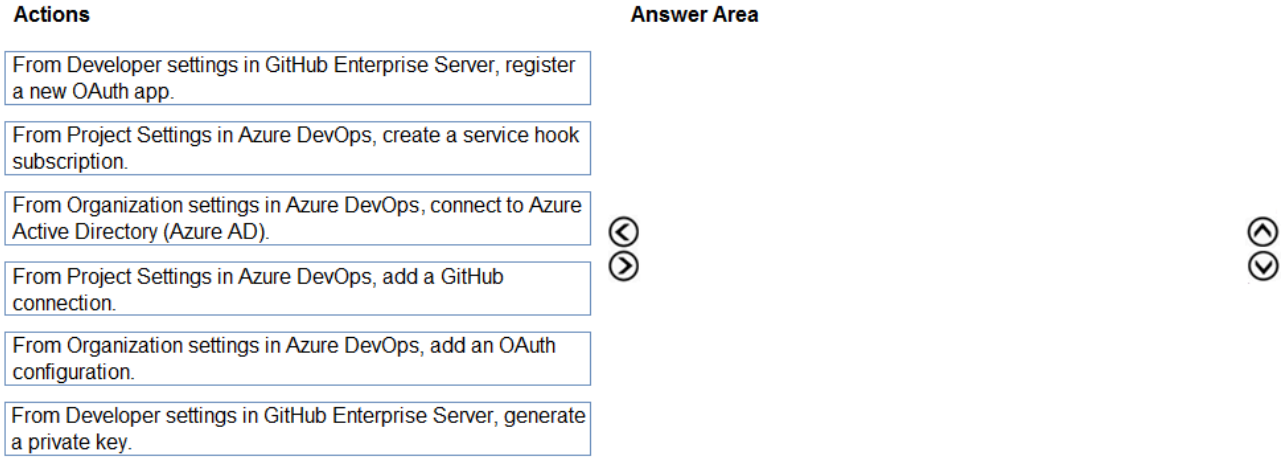
You create an Azure DevOps organization named Contoso.

In the Contoso organization, you create a project named Project1.

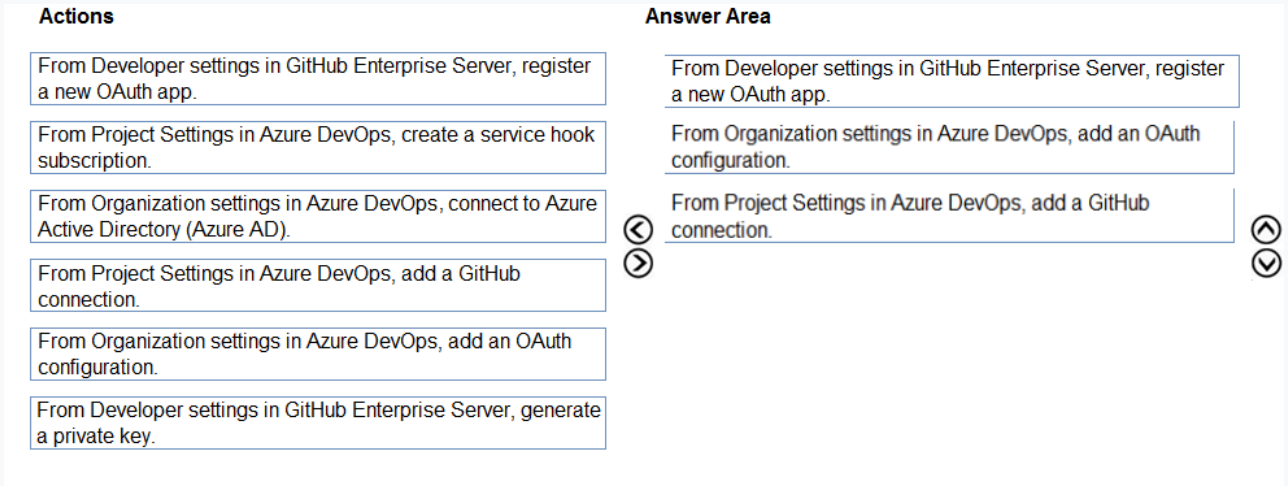
You need to link GitHub commits, pull requests, and issues to the work items of Project1. The solution must use OAuth-based authentication.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Suggested Answer:



Step 1: From Developer settings in GitHub Enterprise Server, register a new OAuth app.

If you plan to use OAuth to connect Azure DevOps Services or Azure DevOps Server with your GitHub Enterprise Server, you first need to register the application as an OAuth App

Step 2: Organization settings in Azure DevOps, add an OAuth configuration

Register your OAuth configuration in Azure DevOps Services.

Note:

1. Sign into the web portal for Azure DevOps Services.
2. Add the GitHub Enterprise Oauth configuration to your organization.
3. Open Organization settings>Oauth configurations, and choose Add Oauth configuration.
4. Fill in the form that appears, and then choose Create.

Step 3: From Project Settings in Azure DevOps, add a GitHub connection.

Connect Azure DevOps Services to GitHub Enterprise Server

Choose the Azure DevOps logo to open Projects, and then choose the Azure Boards project you want to configure to connect to your GitHub Enterprise repositories.

Choose (1) Project Settings, choose (2) GitHub connections and then (3) Click here to connect to your GitHub Enterprise organization.

Reference:

https://docs.microsoft.com/en-us/azure/devops/boards/github/connect-to-github

Sylph Highly Voted 3 years, 5 months ago

Correct, links for each step in answer:
https://docs.microsoft.com/en-us/azure/devops/boards/github/connect-to-github?view=azure-devops#register-azure-devops-in-github-as-an-oauth-app
https://docs.microsoft.com/en-us/azure/devops/boards/github/connect-to-github?view=azure-devops#register-your-oauth-configuration-in-azure-devops-services
https://docs.microsoft.com/en-us/azure/devops/boards/github/connect-to-github?view=azure-devops#connect-azure-devops-services-to-github-enterprise-server

upvoted 21 times

Govcomm Highly Voted 2 years, 1 month ago

GitHub Enterprise Server --> Register an OAuth application
Azure DevOps Organization --> Enable OAuth
Azure DevOps project --> GitHub connection

upvoted 10 times

318touring Most Recent 1 year, 4 months ago

Answer provided in correct
https://learn.microsoft.com/en-us/azure/devops/boards/github/connect-to-github?view=azure-devops#register-azure-devops-in-github-as-an-oauth-app

upvoted 3 times

syu31svc 2 years, 1 month ago

https://docs.microsoft.com/en-us/azure/devops/boards/github/connect-to-github?view=azure-devops#server-github-ent-oauth-register

Answer provided is correct

upvoted 3 times

UnknowMan 2 years, 4 months ago

Correct :

1. Add new Oauth app to GitHub Enterprise
2. From Organization settings, add an OAuth Configuration (Source type: GitHub enterprise)
3. From Project settings, add a new Git Hub Connection

upvoted 2 times

Cheehp 2 years, 5 months ago

Selected during exam.
From Developer settings in GitHub Enterprise Server, register a new OAuth app
Organization settings in Azure DevOps, add an OAuth configuration
From Project Settings in Azure DevOps, add a GitHub connection.

upvoted 1 times

rdemontis 2 years, 6 months ago

correct answer as documentation attached demonstrates

upvoted 2 times

rdemontis 2 years, 5 months ago

to be more precise you can find the solution here:

https://docs.microsoft.com/en-us/azure/devops/boards/github/connect-to-github?view=azure-devops#server-github-ent-oauth-register

upvoted 2 times

SteveChai 3 years, 4 months ago

yes, answer is correct. Verified.

upvoted 7 times

DRAG DROP -

You are configuring an Azure DevOps deployment pipeline. The deployed application will authenticate to a web service by using a secret stored in an Azure key vault.

You need to use the secret in the deployment pipeline.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions	Answer Area
Create a service principal in Azure Active Directory (Azure AD).	
Add an app registration in Azure Active Directory (Azure AD).	
Configure an access policy in the key vault.	
Generate a self-signed certificate.	
Add an Azure Resource Manager service connection to the pipeline.	
Export a certificate from the key vault.	

Suggested Answer:

Actions	Answer Area
Create a service principal in Azure Active Directory (Azure AD).	Create a service principal in Azure Active Directory (Azure AD).
Add an app registration in Azure Active Directory (Azure AD).	Configure an access policy in the key vault.
Configure an access policy in the key vault.	Add an Azure Resource Manager service connection to the pipeline.
Generate a self-signed certificate.	
Add an Azure Resource Manager service connection to the pipeline.	
Export a certificate from the key vault.	

Step 1: Create a service principal in Azure Active Directory (Azure AD).

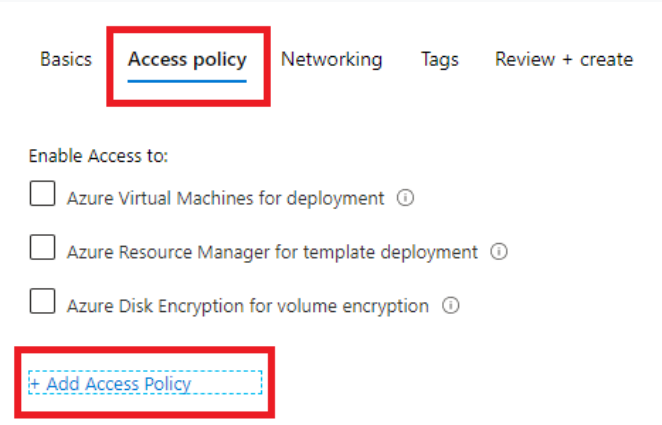
You will need a service principal to deploy an app to an Azure resource from Azure Pipelines.

Step 2: Configure an access policy in the key vault.

You need to secure access to your key vaults by allowing only authorized applications and users. To access the data from the vault, you will need to provide read

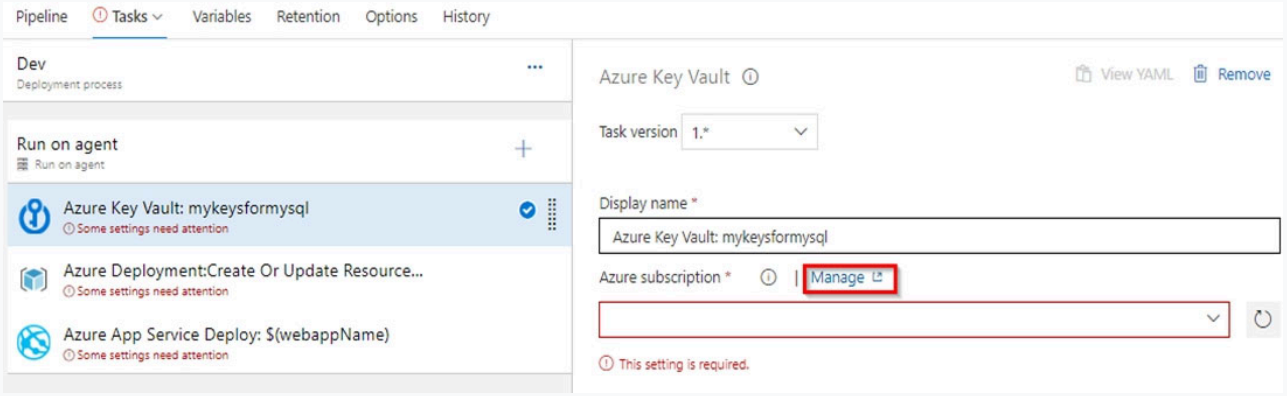
(Get) permissions to the service principal that you will be using for authentication in the pipeline.

Select Access policy and then select + Add Access Policy to setup a new policy.



Step 3: Add an Azure Resource Manager service connection to the pipeline

You need to authorize the pipeline to deploy to Azure:
1. Select Pipelines | Pipelines,
2. Go to Releases under Pipelines and then select and Edit your pipeline.
3. Under Tasks, notice the release definition for Dev stage has a Azure Key Vault task. This task downloads Secrets from an Azure Key Vault. You will need to point to the subscription and the Azure Key Vault resource.
4. Click Manage, this will redirect to the Service connections page.



5.Click on New Service connection -> Azure Resource Manager -> Service Principal (manual). Fill the information from previously created service principal.
Reference:
https://azuredevopslabs.com/labs/vstsextend/azurekeyvault/

erico Highly Voted 3 years, 2 months ago
The answer is correct:
First create a service principal.
Ensure to give the service principal access to the secrets in the kay vault via the access policy
Then Add the Azure Resource Manager service connection which will be used to access the key vault resource.
upvoted 38 times

AzureJobsTillRetire 1 year, 8 months ago
If this is in AZ-500, the answer is definitely wrong. Not sure if it is right in AZ-400 though. I agree with jeet1985 and app registration is the way to go. When you register the app with Azure AD, the service principle is automatically created for the app, and it can either set for RBAC or access policy via Azure portal. When you create a service principle, you will also have to link it to the app. This step is missing in the given answer. Hence, the given answer is not correct.
upvoted 3 times

jeet1985 Highly Voted 3 years, 3 months ago
Answer should be B,C, E

There is no way to directly create a service principal using the Azure portal. When you register an application through the Azure portal, an application object and service principal are automatically created in your home directory or tenant.

https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal
upvoted 38 times

ThomasKong 3 years, 1 month ago
agree with this answer .
upvoted 2 times

lesiris 3 years, 2 months ago
I think this is the right answer https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal#app-registration-app-objects-and-service-principals
upvoted 2 times

lesiris 3 years, 2 months ago
After some thinking not sure about it ... It's written nowhere that the portal is mandatory. We can simply create a service principal using the Azure Cli (az ad sp create-for-rbac). So for me the given answer is correct
upvoted 6 times

KhabibcandefeatGSP 3 years, 2 months ago
This seems like the most correct sequence.
upvoted 1 times

Robert12345Robert 3 years ago
You can: az ad sp create-for-rbac -n ServicePrincipalName
upvoted 7 times

AzureJobsTillRetire 1 year, 8 months ago
This is not correct, as the answer is to use access policy and not rbac for the app
upvoted 1 times

catfood 1 year, 2 months ago
rbac is used to create the service principal. key vault can use either RBAC or access policy, RBAC is recommended
upvoted 1 times

mcabrito Most Recent 6 months, 3 weeks ago
From ChatGPT:

To use a secret stored in an Azure Key Vault in an Azure DevOps deployment pipeline, you would typically perform the following actions in sequence:

Create a service principal in Azure Active Directory (Azure AD):
This service principal will represent the identity that the deployment pipeline will use to access Azure resources, including the Azure Key Vault.
Add an app registration in Azure Active Directory (Azure AD):
Create an app registration in Azure AD associated with the service principal, which will provide the necessary details for authentication.
Configure an access policy in the key vault:
Grant the app registration the necessary permissions (like Get or List) on the secrets stored in the Azure Key Vault.
So, the correct sequence is:

Create a service principal in Azure Active Directory (Azure AD)
Add an app registration in Azure Active Directory (Azure AD)
Configure an access policy in the key vault
upvoted 1 times

varinder82 9 months, 3 weeks ago
Final answer after reading all the comments

- Provided answer by examtopics is right
(Service Principal need to use instead of app registration as app registration only used in web app and here it is not mentioned anywhere)
upvoted 6 times

LindyLou 1 year, 1 month ago
You can not directly create a service principle in AzureAD. To create a service principle for your app, you should register the app in Azure AD.
upvoted 1 times

Yatoom 1 year, 10 months ago
Couldn't you just let the service principal be created automatically when setting up the Azure Resource Manager service connection?
upvoted 6 times

syu31svc 2 years, 1 month ago
Provided answer is correct and provided link supports it
upvoted 1 times

Divyayuvi 2 years, 1 month ago
Why not ?
1. Add an Azure Resource Manager service connection to the pipeline
2. Add an app registration in Azure Active Directory (Azure AD)
3. Configure an access policy in the key vault.

Anyway in the pipeline we need to connect to the Key Vault through Variable group!
upvoted 2 times

Divyayuvi 2 years, 1 month ago

Sorry, its a typo the 2nd point in the above answer should be
2. "Create a service principal"
and not "Add an app registration in Azure Active Directory (Azure AD)"
upvoted 1 times

Govcomm 2 years, 1 month ago
Service Principal --> Access Policy --> ARM service connection
upvoted 4 times

jvyas 2 years, 3 months ago
You can only register app if it is app service. Question doesn't state where the app has been deployed, so SP makes more sense than app registration
upvoted 1 times

UnknowMan 2 years, 4 months ago
Create a service principal
Give access to KV via access policy (Use the SP created)
Add Arm service to pipeline
upvoted 1 times

somenkr 2 years, 5 months ago
Answer should be B,C, E
There is no way to directly create a service principal using the Azure portal. When you register an application through the Azure portal, an application object and service principal are automatically created in your home directory or tenant.
upvoted 3 times

resonant 1 year, 2 months ago
As lesiris told jeet1985:
"It's written nowhere that the portal is mandatory. We can simply create a service principal using the Azure Cli (az ad sp create-for-rbac). So for me the given answer is correct."
upvoted 1 times

resonant 1 year, 2 months ago
My bad. I just discovered this and apparently the application would be automatically created with the Azure CLI command and you'd have to do it with Powershell instead: https://stackoverflow.com/a/71613311/5744858. It seems weird that the behaviour of Azure CLI and Powershell would vary like this. Please someone confirm the StackOverflow post is right and only the Powershell command would create the service principal without creating an app.
upvoted 1 times

shubhb11 2 years, 5 months ago
There is no way to directly create a service principal using the Azure portal. When you register an application through the Azure portal, an application object and service principal are automatically created in your home directory or tenant.
https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal#app-registration-app-objects-and-service-principals

create App registration
upvoted 1 times

resonant 1 year, 2 months ago
You can create a service principal without the Azure Portal and without creating an application first:
https://stackoverflow.com/a/71613311/5744858
upvoted 1 times

rdemontis 2 years, 6 months ago
the answer is correct as demonstrated by the attached documentation
upvoted 2 times

lugospod 2 years, 7 months ago
Got this January 2022.
upvoted 3 times

[Removed] 2 years, 9 months ago
The App registration is the template used to create the SP. The SP is a security principal (like a User) which can be authenticated and authorised

So the most common way of doing this is creating app registration, this is also where you will get a service principal, you use that app/sp for a policy in a key vault, and then as a last step you use this SP in a pipeline

upvoted 1 times

ingAlfano 3 years, 1 month ago

when you create a new service connection you create a service principal as well.

If you already have service connection you already have a service principal so I don't see the point of creating a service principal here..

upvoted 2 times

ingAlfano 3 years, 1 month ago

Then there is not any clue the app will run on azure so no need to deploy to azure..

upvoted 1 times

Question #26 *Topic 4*

DRAG DROP -

You have a private project in Azure DevOps and two users named User1 and User2.

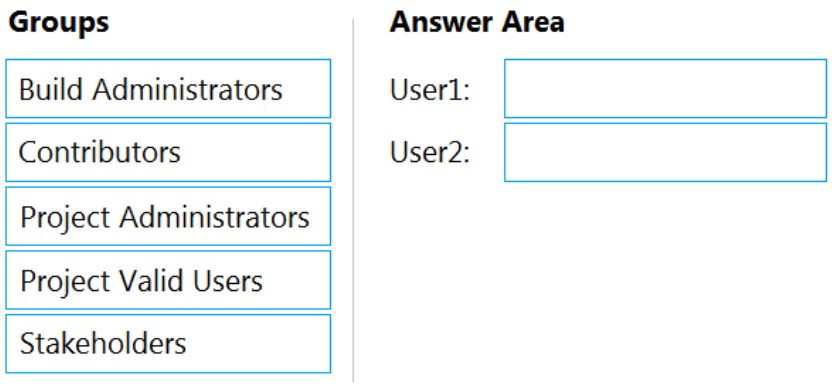
You need to add User1 and User2 to groups to meet the following requirements:

- User1 must be able to create a code wiki.
- User2 must be able to edit wiki pages.
- The solution must use the principle of least privilege.

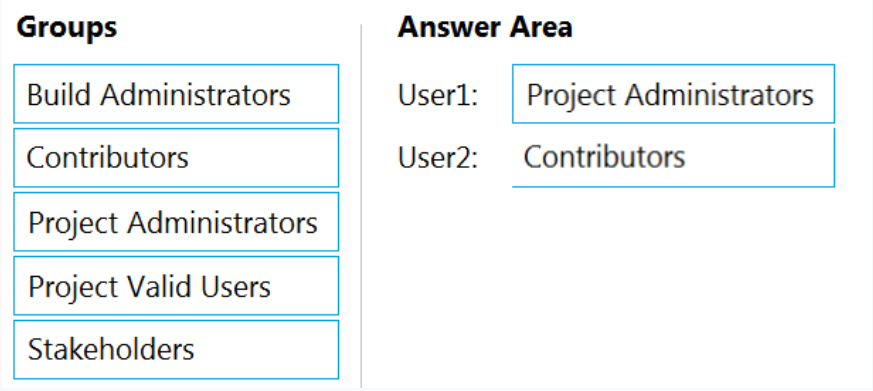
To which group should you add each user? To answer, drag the appropriate groups to the correct users. Each group may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested Answer:



User1: Project Administrators -

You must have the permission Create Repository to publish code as wiki. By default, this permission is set for members of the Project Administrators group.

User2: Contributors -

Anyone who is a member of the Contributors security group can add or edit wiki pages.

Anyone with access to the team project, including stakeholders, can view the wiki.

Reference:

https://docs.microsoft.com/en-us/azure/devops/project/wiki/wiki-create-repo

Sylph Highly Voted 3 years, 5 months ago

Correct

upvoted 18 times

francis6170 Highly Voted 3 years, 2 months ago

Got this in the AZ-400 exam (June 2021).

upvoted 15 times

Christian_garcia_martin Most Recent 2 weeks, 6 days ago

with the requirement of principle of least privilege User1 could be perfectly Contributor .

User1 -> Contributors

User2 -> Contributors

upvoted 1 times

ozbonny 6 months, 3 weeks ago
Correct
upvoted 1 times

Smalec44 11 months, 3 weeks ago
from the link provided, so yes answer is correct:

You must have the permission Create Repository to publish code as wiki. By default, this permission is set for members of the Project Administrators group.
Anyone who is a member of the Contributors security group can add or edit wiki pages. Anyone with access to the team project, including stakeholders, can view the wiki.
upvoted 2 times

Sukon_Desknot 1 year ago
The answers should both be "Wiki Contributors"
upvoted 2 times

maurizio2471 1 year, 4 months ago
Correct

You must have the permission Create Repository to publish code as wiki. By default, this permission is set for members of the Project Administrators group.
Anyone who is a member of the Contributors security group can add or edit wiki pages. Anyone with access to the team project, including stakeholders, can view the wiki.

https://learn.microsoft.com/en-us/azure/devops/project/wiki/wiki-create-repo?view=azure-devops&tabs=browser#prerequisites
upvoted 1 times

Sukon_Desknot 1 year, 1 month ago
Incorrect, Contributors and Project Admins can both create wikis therefore, with principle of least privilege, the answer should Contributor and Contributor
upvoted 2 times

Tyler2023 1 year ago
I don't think so, if you open the link above and read it, from maurizio2471, to publish code as wiki. By default, this permission is set for members of the Project Administrators group.
upvoted 1 times

reks2022 1 year, 9 months ago
Contributor,Contributor as least privilege access
learn.microsoft.com/en-us/azure/devops/organizations/security/permissions-access?toc=%2Fazure%2Fdevops%2Fproject%2Ftoc.json&view=azure-devops
upvoted 14 times

Yatoom 1 year, 10 months ago
I think it should be "Contributors" and "Contributors".

Contributors can publish code as a wiki:
https://learn.microsoft.com/en-us/azure/devops/organizations/security/permissions-access?view=azure-devops#notifications-alerts-and-team-collaboration-tools

By default, all project contributors have read and edit access of the wiki repository:
https://learn.microsoft.com/en-us/azure/devops/project/wiki/manage-readme-wiki-permissions?view=azure-devops
upvoted 5 times

syu31svc 2 years, 1 month ago
Provided answer is correct and supported by link given
upvoted 1 times

sha1979 2 years, 1 month ago
Clarification, Contributors = Members of this group can add, modify, and delete items within the team project.
Project Administrators = Members of this group can perform all operations in the team project.
upvoted 1 times

Govcomm 2 years, 1 month ago
Project administrator --> Contributor
upvoted 1 times

rdemontis 2 years, 6 months ago
Correct answer.
upvoted 1 times

Art3 2 years, 8 months ago
Correct
upvoted 1 times

malikimran21 2 years, 9 months ago
this came in today exam Az-400 (Dec 2021)
upvoted 1 times

subrata83 2 years, 11 months ago
Got this in the Az-400 exam(Sep 27 2021)
upvoted 3 times

V_Ramon 3 years, 1 month ago
this question came out today, July 28, 2021
upvoted 3 times

Question #27 *Topic 4*

You use WhiteSource Bolt to scan a Node.js application.
The WhiteSource Bolt scan identifies numerous libraries that have invalid licenses. The libraries are used only during development and are not part of a production deployment.
You need to ensure that WhiteSource Bolt only scans production dependencies.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Run npm install and specify the --production flag.

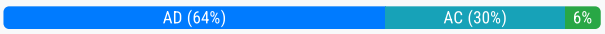
B. Modify the WhiteSource Bolt policy and set the action for the licenses used by the development tools to Reassign.

C. Modify the devDependencies section of the project's Package.json file.

D. Configure WhiteSource Bolt to scan the node_modules directory only.

Suggested Answer: *AC*
A: To resolve NPM dependencies, you should first run "npm install" command on the relevant folders before executing the plugin.
C: All npm packages contain a file, usually in the project root, called package.json ว€" this file holds various metadata relevant to the project. This file is used to give information to npm that allows it to identify the project as well as handle the project's dependencies. It can also contain other metadata such as a project description, the version of the project in a particular distribution, license information, even configuration data ว€" all of which can be vital to both npm and to the end users of the package.
Reference:
https://whitesource.atlassian.net/wiki/spaces/WD/pages/34209870/NPM+Plugin https://nodejs.org/en/knowledge/getting-started/npm/what-is-the-file-package-json

Community vote distribution



rdemontis Highly Voted 2 years, 6 months ago

Selected Answer: AD

Correct answers are A & D.
1. When you use --production flag in npm install devDependencies are not installed (so C is wrong).
2. npm install command installs the dependencies to the local node_modules folder.

https://docs.npmjs.com/cli/v8/commands/npm-install

3. WhiteSource scan the entire project folder by default. You have to configure it to scan only the node_modules since the production dependencies are there.

https://whitesource.atlassian.net/wiki/spaces/WD/pages/33751265/Previous+Version+of+WhiteSource+Bolt+for+Azure+Pipeline#Build-Configuration-for-Azure-DevOps-Server

"If there is a policy match on a Reassign action, the request will be automatically reassigned to a designated user or group in the system which is not the default approver."

https://whitesource.atlassian.net/wiki/spaces/WD/pages/34013519/Managing+Automated+Policies#Applying-Actions-to-a-Library

But is this action required in the question? Of course no. So even B is wrong
upvoted 23 times

cluqueg 1 year, 4 months ago
This is a very tricky approach and it's not the best solution at all.
upvoted 2 times

27close Highly Voted 3 years, 10 months ago
the answer is correct - devDependent and productionflag
upvoted 19 times

ravikrg 1 year, 11 months ago

I think, devDependencies and productionflag are interlinked
when we add devDependencies and during installation add the productionflag the devDependencies will not be installed.

And coming to option D, if we are using productionflag why do we need to configure the whitesource to look at node_modules folder, isn't it obvious that node_modules is where the packages are installed? why do we need to exclusively set to look at node_modules?

My answer would be CA in sequence. Please correct me if I am wrong

upvoted 1 times

nakedsun 1 year, 6 months ago

Answer is correct, not sure what everyone else is smoking, guess there are not many Node devs here. How will Whitesource/Mend know which deps are for develpoment unless we modify packakge.json and assign the dev dependancies, is it just going to guess?

Then we need to make sure the npm install/build process uses --production so it doesn't pull the development deps. Then the scan is run (assumed to be during a pipline build) on only production deps in node_modules.

upvoted 6 times

Mattt Most Recent 4 months ago

Selected Answer: AC

First C : We should first move the dev packages to the devDependencies
Then A : npm install --production

upvoted 2 times

ozbonny 6 months, 3 weeks ago

Selected Answer: AC

I think I'll go by A and C since the question says 'The libraries are used only during development and are not part of a production deployment.' it means that you need to add the dev dependencies in your Package.json file.

upvoted 4 times

DGladiator 1 year, 4 months ago

A. Run npm install and specify the --production flag. This will make npm only install the dependencies listed in the "dependencies" section of your package.json and skip those listed in the "devDependencies" section, which are assumed to be only relevant for development purposes. Therefore, only production dependencies will be present in the node_modules directory for WhiteSource Bolt to scan.

D. Configure WhiteSource Bolt to scan the node_modules directory only. By focusing the scan to the node_modules directory, you ensure that WhiteSource Bolt only considers packages that have been installed and are needed for production. It would not take into account those packages which are purely for development purposes and thus not present in this directory.

upvoted 3 times

cluqueg 1 year, 4 months ago

Selected Answer: AC

AC is the correct and enforces an smart definition of run-time and development deps.

upvoted 3 times

mmdex 1 year, 8 months ago

Selected Answer: AC

I'd say the answer AC is correct. You need to modify devDependencies in package.json (C) so that npm knows which dependencies are for development use only, and run install with --production flag (A) to not install them.

I do not see how D would help me. Both production and development dependencies are installed in the same "node_modules" folder. Restricting WhiteSource to scan only this folder would not exclude development dependencies.

upvoted 6 times

AzureJobsTillRetire 1 year, 8 months ago

This answer makes the most sense to me so far. I think we need both production and development and not production only.

upvoted 1 times

meoukg 1 year, 10 months ago

A & D were my chosen answers yesterday when I sat on this exam and I passed

upvoted 6 times

syu31svc 2 years, 1 month ago

Selected Answer: AD

npm install is what you need to do so A is correct

https://stackoverflow.com/questions/72784118/unable-resolve-npm-dependencies-while-whitesource-scan-in-jenkins

"doing whitesource scan for node_modules directory and when scanning ,in resolving dependency"

Taking D as the other answer

upvoted 3 times

tjeerd 2 years, 1 month ago

Selected Answer: AD

On exam 20220727.

upvoted 6 times

UnknowMan 2 years, 4 months ago

AB

C is strange... we dont want to update our dev dependencies to valid our prod dependencies..

upvoted 1 times

Cheehp 2 years, 5 months ago

Selected during exam.

A. Run npm install and specify the --production flag.

B. Modify the WhiteSource Bolt policy and set the action for the licenses used by the development tools to Reassign.

upvoted 2 times

SoftwareEngineeringMaster 2 years, 3 months ago

Ok, what your score or percentage of area you need improve it.

upvoted 1 times

AlexLiourtas 2 years, 5 months ago

Selected Answer: AB

Tested

upvoted 1 times

debleenac85 2 years, 5 months ago

B is an independant option. We do not have to do Step A, if we do Step B. Here the question mentions part of solution. So AD will be the answer.

upvoted 2 times

jasifu3 2 years, 6 months ago

Selected Answer: AB

so I guess people are just upvoting the most upvoted answer because it's usually correct? In this case it's clearly wrong. Modifying devDependencies will modify... your development dependencies. Which is undesirable. Here we just want to change what whitesource does.

upvoted 2 times

prashantjoge 2 years, 5 months ago

Eash answer represents part of the problem. So it is correct

upvoted 1 times

prashantjoge 2 years, 5 months ago

what reassign does - Reassign the request to a designated user or group in the system which is not the default approver.

upvoted 1 times

jasifu3 2 years, 6 months ago

actually, the answer may be AD, since npm install with the production flag will ensure that only prod dependencies are in node_modules. IDK the details of how whitesource works though - if it usually looks elsewhere then node_modules too.

upvoted 4 times

pengyanb 2 years, 7 months ago

A and B are correct.

https://whitesource.atlassian.net/wiki/spaces/WD/pages/34013519/Managing+Automated+Policies

upvoted 3 times

pengyanb 2 years, 7 months ago

C doesn't make any sense. Why do you need to modify the devDepenedency????

npm install with --production flag will only install the prod dependency, whatever is specified in the "devDependency" is not relevant.

upvoted 3 times

malikimran21 2 years, 9 months ago

this came in today exam Az-400 (Dec 2021)

upvoted 3 times

Question #28 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You plan to update the Azure DevOps strategy of your company.

You need to identify the following issues as they occur during the company's development process:

➩ Licensing violations

➩ Prohibited libraries

Solution: You implement continuous integration.

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*

WhiteSource is the leader in continuous open source software security and compliance management. WhiteSource integrates into your build process, irrespective of your programming languages, build tools, or development environments. It works automatically, continuously, and silently in the background, checking the security, licensing, and quality of your open source components against WhiteSource constantly-updated definitive database of open source repositories.

Reference:

https://azuredevopslabs.com/labs/vstsextend/whitesource/

Community vote distribution

B (65%) A (35%)

quokka Highly Voted 4 years ago

B. No. CI by itself won't address the issues.

upvoted 50 times

MMM123 3 years, 8 months ago

I don't agree with you. Explanation of the answer in ExamTopics seems reasonable. WhiteSource is a CI

upvoted 5 times

ThePenalty 3 years, 8 months ago

Then login to Azure Devops could also be the right answer, because it is part of the solution.

upvoted 31 times

deepakjuneja 2 years, 11 months ago

Penetration testing comes under CI not WhiteSource which comes during development, build Pipelines ... hence correct answer is No

upvoted 2 times

tom999 3 years, 7 months ago

You can integrate WhiteSource into your CI pipeline as it is done in the lab referenced in the explanation.

But implementing CI could be also done with a build task or build+test or build+test+code analysis or ...

So the answer is "B = No"

upvoted 14 times

JimmyC Highly Voted 3 years, 4 months ago

This answer should be No. Although Whitesource can be added to the CI build, simply enabling CI will not at all have the required effect. The answer doesn't mention Whitesource Bolt at all - only the examtopics explanation talks about Whitesource Bolt (and doesn't even mention CI once). This answer makes no sense.

upvoted 12 times

dba7x 3 years, 3 months ago

Read again and you will see that it says "You implement CI", so we should believe that they implemented it correctly and it addresses the issue.

upvoted 1 times

jasifu3 2 years, 6 months ago

by this logic almost any solution would lead to a yes, because we can assume that the necessary steps to achieve the goal was taken even though it wasn't mentioned....

upvoted 4 times

ozbonny Most Recent 6 months, 3 weeks ago

Selected Answer: B

I think is B since the question says 'You plan to update the Azure DevOps strategy of your company.' so I think it infers that some build pipeline was created so now you need to configure the Whitesource bolt

upvoted 1 times

hardinxcore 8 months, 3 weeks ago

Selected Answer: B

Just continuous integration isn't enough to meet the goal. The answer really needs to be more specific, i.e. what kind of CI?

upvoted 1 times

flafernan 1 year ago

Selected Answer: B

B- Não. Implementing continuous integration alone does not directly resolve issues of licensing violations or the use of prohibited libraries. Continuous integration is a practice that involves automating builds and tests to ensure that code is always ready for deployment.

To address the issues of license violations and banned libraries, you often need to add additional tools or processes such as static code analysis, dependency checking, and license checking.

upvoted 1 times

Pukun 1 year, 3 months ago

The Answer Should be "NO"

upvoted 1 times

DGladiator 1 year, 4 months ago

GPT4

No, this does not meet the goal.

Implementing continuous integration (CI) in and of itself does not inherently identify licensing violations or prohibited libraries. Continuous integration is a practice in software development where developers regularly merge their changes into a main branch, often triggering automated build and test processes.

To identify licensing violations and prohibited libraries, you'd typically use a software composition analysis (SCA) tool. An SCA tool analyzes the open source components of your software for security vulnerabilities, licensing compliance, and more. An example of such a tool could be WhiteSource Bolt, Sonatype, or BlackDuck. These tools can be incorporated into your CI pipeline to check every build for these issues.

upvoted 1 times

cluqueg 1 year, 4 months ago

Selected Answer: A

Mend will handle both reqs. and the recommended step to run it is on CI.

https://learn.microsoft.com/en-us/training/modules/introduction-to-secure-devops/5-explore-key-validation-points?pivots=portal

upvoted 1 times

cluqueg 1 year, 4 months ago

Selected Answer: B

It's a very clear No.

upvoted 1 times

PlatyPlatypus 2 years, 1 month ago

Selected Answer: B

Should be a No because CI itself doesn't necessarily include WhiteSource it could mean anything

upvoted 3 times

syu31svc 2 years, 1 month ago

Selected Answer: B

I would go with No as the answer

You need security scanning

upvoted 2 times

Divyayuvi 2 years, 1 month ago

Selected Answer: A

It should be Yes

upvoted 2 times

Govcomm 2 years, 1 month ago

Continuous Integration as part of the build pipeline --> WhiteSource so it is YES.

upvoted 1 times

UnknowMan 2 years, 4 months ago

This answer should be No, CI is not the solution.

CI + WhiteSource is the solution

upvoted 2 times

rdemontis 2 years, 6 months ago

Selected Answer: A

I think the answer provided is correct even though it is very general. In fact however tools like WhiteSource Bolt or Black Duck are used in the Continuos Integration process, so it is correct to implement it. Indubitably it would be desirable to have more precise answers.

upvoted 4 times

jose 1 year, 9 months ago

I agree. I think the key is the word "strategy":

"You plan to update the Azure DevOps strategy of your company".

The stretegy would be to implement continuous integration and as part of that strategy you can use tools lik WhiteSource.

upvoted 2 times

Gluckos 2 years, 7 months ago

Selected Answer: B

Agree with this

upvoted 4 times

poplovic 3 years, 1 month ago

If considering this question with others in a bundle, this CI solution is the most correct.

1. you need WhiteSource or DarkDuck to scan
2. WhiteSource or DarkDuke is integrated in CI
3. Therefore, if you implement CI, it is possible to achieve the goal

I tend to agree with "A"--Yes

upvoted 2 times

xRiot007 1 year, 2 months ago

Yes and No. A CI pipeline is not required to have static analysis and will run very well without them. SCA tools are also not contained in a CI/CD pipeline by default. The answer to this question is ambiguos in the most.

upvoted 1 times

Question #29 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You plan to update the Azure DevOps strategy of your company.
You need to identify the following issues as they occur during the company's development process:
➩ Licensing violations
➩ Prohibited libraries
Solution: You implement pre-deployment gates.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Instead use implement continuous integration.
Note: WhiteSource is the leader in continuous open source software security and compliance management. WhiteSource integrates into your build process, irrespective of your programming languages, build tools, or development environments. It works automatically, continuously, and silently in the background, checking the security, licensing, and quality of your open source components against WhiteSource constantly-updated definitive database of open source repositories.
Reference:
https://azuredevopslabs.com/labs/vstsextend/whitesource/

Community vote distribution

B (100%)

ScreamingHand Highly Voted 3 years, 1 month ago
I like the quick & easy ones
upvoted 8 times

syu31svc Most Recent 2 years, 1 month ago
Selected Answer: B
No is the answer

https://docs.microsoft.com/en-us/azure/devops/pipelines/release/approvals/?view=azure-devops

A team wants to ensure there are no active issues in the work item or problem management system before deploying a build to a stage --> Pre-deployment gates
upvoted 1 times

syu31svc 2 years, 1 month ago
Disregard my previous post; completely irrelevant to the question

Answer is No (in any case) as security scanning is needed
upvoted 1 times

UnknowMan 2 years, 4 months ago
Selected Answer: B
This answer should be No.

We can check on a gate, but the real solution is to Add WhiteSource on CI
And maybe use gates to block the process.
But with just a gate we can do nothink
upvoted 3 times

prashantjoge 2 years, 5 months ago

https://www.azuredevopslabs.com/labs/vstsextend/releasegates/#:~:text=Pre-deployment%20gates%20ensures%20there%20are%20no%20active%20issues,before%20promoting%20the%20release%20to%20the%20next%20environme

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: B

correct answer

upvoted 1 times

goatlord 3 years, 1 month ago

Hypothetically, could you use pre-deployment gates to check for licenses?
Of course, it's a bad methodology... but you could do it?

upvoted 1 times

ChewyLife 2 years, 4 months ago

But the task is to identify. Gates are for blocking.

upvoted 4 times

Dady9 3 years, 5 months ago

shouldn't be Yes?

upvoted 1 times

noussa 3 years, 4 months ago

the given answer is Correct. it should be No cause it's not the role of pre-deployment gates to check for your licenses
Pre-deployment gates ensure there are no active issues in the work item or problem management system before deploying a build to an environment.

upvoted 8 times

Question #30 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You plan to update the Azure DevOps strategy of your company.

You need to identify the following issues as they occur during the company's development process:

➩ Licensing violations

➩ Prohibited libraries

Solution: You implement automated security testing.

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Instead use implement continuous integration.

Note: WhiteSource is the leader in continuous open source software security and compliance management. WhiteSource integrates into your build process, irrespective of your programming languages, build tools, or development environments. It works automatically, continuously, and silently in the background, checking the security, licensing, and quality of your open source components against WhiteSource constantly-updated definitive database of open source repositories.

Reference:

https://azuredevopslabs.com/labs/vstsextend/whitesource/

Community vote distribution

JimmyC Highly Voted 3 years, 4 months ago

IMO this is the correct answer (it should be Yes). I've already explained in the previous answer why Continuous Integration is wrong, and that Whitesource Bolt is not necessarily part of CI. However, Whitesource Bolt *IS* an automated security testing solution (which is added to the build pipeline). This answer is more specific, and more correct, than the CI answer.

upvoted 58 times

CyberLumi 3 years, 3 months ago

I agree with you Jimmy

upvoted 3 times

60ties Most Recent 2 months ago

Selected Answer: B

Answer is B. Licensing violation is not a code security issue. It is a legal issue. The "solution: You implement automated security testing." is for code testing & not legalities.

upvoted 2 times

UrbanRellik 4 months ago

Selected Answer: A

WhiteSource, Mend Bolt supports automated security testing when integrated into a CI pipeline.

upvoted 1 times

Mattt 4 months ago

Selected Answer: B

B is correct

upvoted 1 times

4bd3116 4 months, 3 weeks ago

Selected Answer: A

Automated Security Testing:

Set up automated security testing in your CI/CD pipeline.

Use tools like WhiteSource Bolt or Snyk to scan your codebase for vulnerabilities, security risks, and licensing issues.
Configure Licensing Compliance Checks:
Ensure that your automated tests also verify licensing compliance.
Address any licensing violations or prohibited libraries promptly.
upvoted 2 times

chloaus 5 months, 1 week ago
A. Here is an example: https://www.synopsys.com/software-integrity/software-composition-analysis-tools/black-duck-sca.html
upvoted 1 times

AymanAkk 1 year ago
Selected Answer: A
answer is A
upvoted 1 times

Ret2Me 1 year ago
Selected Answer: B
In my opinion licensing violation is not mandatory part of the security test
upvoted 3 times

Sukon_Desknot 1 year, 1 month ago
Selected Answer: B
The answer is B, security testing can be implemented and it still won't check the issue of prohibited libraries or licensing issues
upvoted 1 times

flafernan 1 year, 1 month ago
Selected Answer: B
B - No. Implementing automated security testing does not specifically address the issues of licensing violations and prohibited libraries. While automated security testing is important for identifying vulnerabilities and security issues in code, it is not focused on issues related to licenses and libraries.
upvoted 2 times

flafernan 1 year, 1 month ago
B - No. Implementing automated security testing does not specifically address the issues of licensing violations and prohibited libraries. While automated security testing is important for identifying vulnerabilities and security issues in code, it is not focused on issues related to licenses and libraries.
upvoted 1 times

catfood 1 year, 2 months ago
Selected Answer: B
licencing issues isn't security scanning....

"finding and fixing open source vulnerabilities" using mend bolt, yes that would likely come under security scanning.
upvoted 2 times

DGladiator 1 year, 4 months ago
GPT4
Yes, implementing automated security testing with the right tools could meet the goal, but only partially. Automated security testing can help identify security vulnerabilities in your software, but on its own, it may not be fully equipped to identify licensing violations or usage of prohibited libraries.
upvoted 1 times

Mcs_ 1 year, 4 months ago
No, this does not meet the goal. Automated security testing can help identify some security issues in the code, such as vulnerabilities, misconfigurations, or malicious code. However, automated security testing cannot detect licensing violations or prohibited libraries, which are related to the legal and compliance aspects of using open-source software. To identify these issues, you need to use a tool that can scan the open-source components and their licenses in your application, such as WhiteSource Bolt.
upvoted 3 times

dmt6263 1 year, 5 months ago
Selected Answer: A
From ChatGPT:

Implementing automated security testing can help to address the identified issues of licensing violations and prohibited libraries.

Automated security testing involves running automated tests that check for security vulnerabilities, such as those related to licensing or the use of prohibited libraries, in the code. By implementing this practice, the company can detect security issues early in the development process, allowing them to be addressed before the code is deployed to production.

Implementing continuous integration alone does not directly address the identified issues of licensing violations and prohibited libraries.

Continuous integration is a software development practice that involves automatically building, testing, and integrating code changes into a shared repository multiple times a day. This practice can help detect issues early in the development process and ensure that code changes do not break the application.
upvoted 2 times

catfood 1 year, 1 month ago
i wish people would stop posting chat GPT. Its confidently wrong on many things. Go read the microsoft documentation
upvoted 4 times

nakedsun 1 year, 6 months ago
Selected Answer: B
"Licensing violations" is nothing to do with security, and "Prohibited libraries" is debateable, could be security if it is prohibitied due to vulnerability, or could be prohibited due to company policy.

The CI option from a previous question makes far more sense.
upvoted 2 times

xRiot007 1 year, 2 months ago
Why ? CI does not require static scanning to be done.
upvoted 1 times

surensaluka 1 year, 8 months ago
Selected Answer: B
https://www.braindump2go.com/free-online-pdf/AZ-400-PDF(178-188).pdf
I checked another dump as well. The answer is aligned with examtopics.
upvoted 1 times

resonant 1 year, 2 months ago
I wouldn't trust answers from most dumps because I have understood they only copy questions and answers from each other. ExamTopics might copy from braindump2go, braindump2go might copy the dumps from somewhere else, etc.
upvoted 1 times

Question #31 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You plan to update the Azure DevOps strategy of your company.

You need to identify the following issues as they occur during the company's development process:

➩ Licensing violations

➩ Prohibited libraries

Solution: You implement continuous deployment.

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Instead implement continuous integration.

Note: WhiteSource is the leader in continuous open source software security and compliance management. WhiteSource integrates into your build process, irrespective of your programming languages, build tools, or development environments. It works automatically, continuously, and silently in the background, checking the security, licensing, and quality of your open source components against WhiteSource constantly-updated definitive database of open source repositories.

Reference:

https://azuredevopslabs.com/labs/vstsextend/whitesource/

Community vote distribution

B (100%)

manojsb Highly Voted 3 years, 4 months ago

no is correct

upvoted 6 times

syu31svc Most Recent 2 years, 1 month ago

Selected Answer: B

100% is no

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: B

correct

upvoted 1 times

Kalaismile06 3 years, 3 months ago

Repeated question. Given answer is correct.

upvoted 4 times

Question #32 *Topic 4*

SIMULATION -

You manage a website that uses an Azure SQL Database named db1 in a resource group named RG1lod11566895.

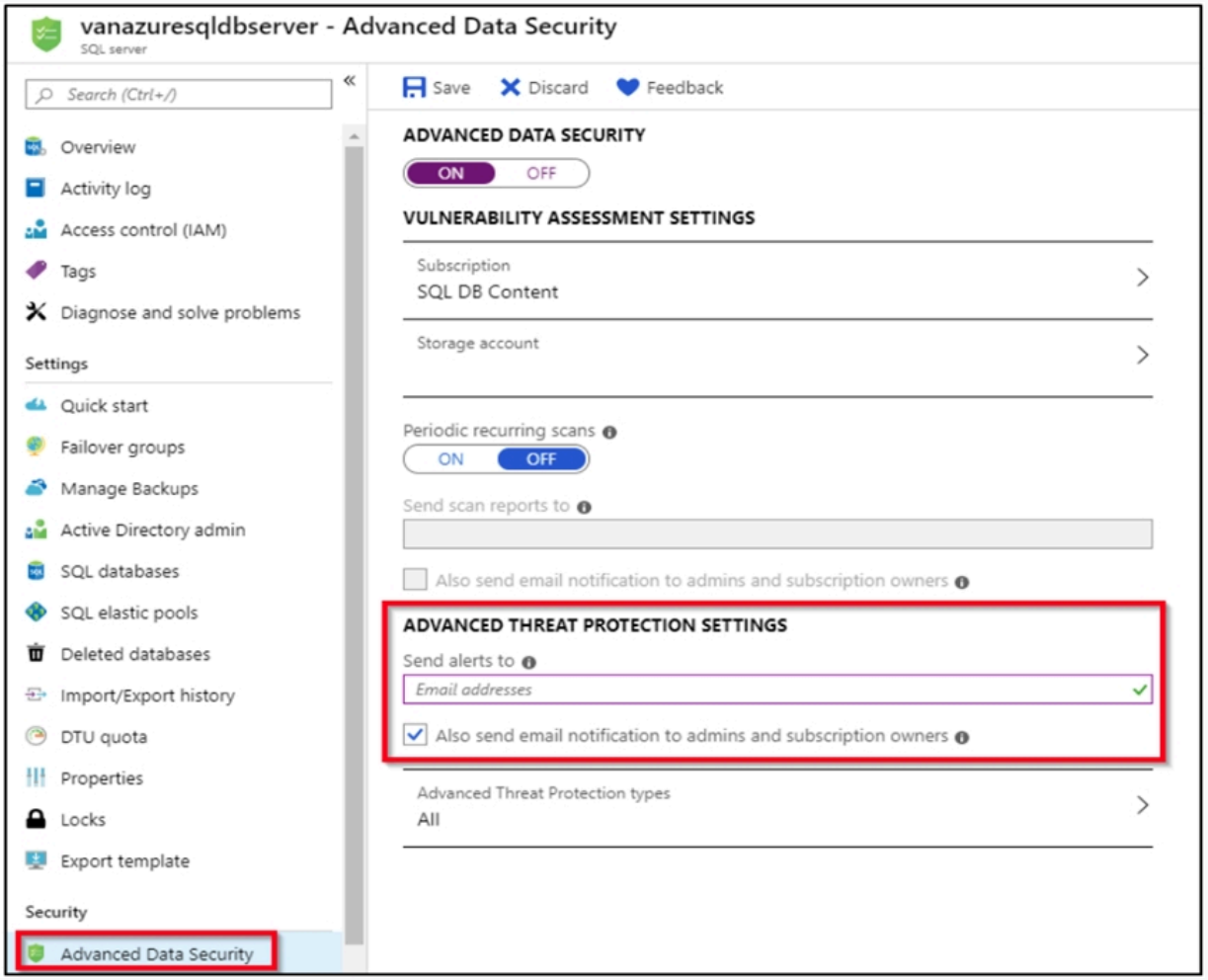
You need to modify the SQL database to protect against SQL injection.

To complete this task, sign in to the Microsoft Azure portal.

Suggested Answer: *See explanation below.*

Set up Advanced Threat Protection in the Azure portal

1. Sign into the Azure portal.
2. Navigate to the configuration page of the server you want to protect. In the security settings, select Advanced Data Security.
3. On the Advanced Data Security configuration page:



4. Enable Advanced Data Security on the server.

Note: Advanced Threat Protection for Azure SQL Database detects anomalous activities indicating unusual and potentially harmful attempts to access or exploit databases. Advanced Threat Protection can identify Potential SQL injection, Access from unusual location or data center, Access from unfamiliar principal or potentially harmful application, and Brute force SQL credentials

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/storage-account-create https://docs.microsoft.com/en-us/azure/azure-sql/database/threat-detection-configure

meinekarte Highly Voted 3 years, 5 months ago

From the Azure portal, open your server or managed instance.

Under the Security heading, select Security Center.

Select Enable Azure Defender for SQL.

https://docs.microsoft.com/en-us/azure/azure-sql/database/azure-defender-for-sql#enable-azure-defender-for-azure-sql-database-at-the-resource-level

upvoted 24 times

kumud 3 years, 1 month ago

correct

upvoted 1 times

rdemontis 2 years, 5 months ago

correct

upvoted 1 times

waqas 2 years, 5 months ago

From the Azure portal, open your server or managed instance.
Under the Security heading, select Defender for Cloud.
Select Enable Microsoft Defender for SQL.

upvoted 5 times

PlumpyTumbler Highly Voted 2 years, 7 months ago

The Azure Portal interface is changing all the time. The given answer and all comments so far are obsolete as of 1/24/22. Because of that, don't expect to see a simulation like this on the exam. However, if you want to follow the trail of breadcrumbs to accomplish this:

Under security in your Azure SQL DB, click "Microsoft Defender for Cloud"
The click "View all recommendations in defender for cloud"
Expand "Enable enhanced security features"
Click "Microsoft Defender for Azure SQL Database servers should be enabled"
At the top of the page click "Enforce"
In the Scope section: assign the resource group from the question
To finish, click select or create or whatever the blue button says at the time you are viewing this and you're done.

Keep in mind, that by 3/1/22 this could be obsolete as well because the portal changes all the time.

upvoted 16 times

PlumpyTumbler 2 years, 7 months ago

https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-sql-introduction?wt.mc_id=defenderforcloud_inproduct_portal_recoremediation&WT.mc_id=Portal-Microsoft_Azure_Security

upvoted 2 times

ozbonny Most Recent 6 months, 3 weeks ago

From the Azure portal, open your server or managed instance.
Under the Security heading, select Defender for Cloud.
Select Enable Microsoft Defender for SQL.

upvoted 2 times

Tyler2023 1 year ago

You can follow this instructions: https://learn.microsoft.com/en-us/azure/azure-sql/database/threat-detection-configure?view=azuresql
Configure Advanced Threat Protection for Azure SQL Database

Advanced Threat Protection for Azure SQL Database detects anomalous activities indicating unusual and potentially harmful attempts to access or exploit databases. Advanced Threat Protection can identify Potential SQL injection, Access from unusual location or data center, Access from unfamiliar principal or potentially harmful application, and Brute force SQL credentials - see more details in Advanced Threat Protection alerts.

You can receive notifications about the detected threats via email notifications or Azure portal

Advanced Threat Protection is part of the Microsoft Defender for SQL offering, which is a unified package for advanced SQL security capabilities. Advanced Threat Protection can be accessed and managed via the central Microsoft Defender for SQL portal.

upvoted 1 times

yana_b 1 year, 1 month ago

Detailed steps for enabling on the defender on both subscription and resource level can be found here:
https://learn.microsoft.com/en-us/azure/azure-sql/database/azure-defender-for-sql?view=azuresql

upvoted 2 times

yana_b 1 year, 1 month ago

As per my understanding, the question refers to enabling the defender on resource level and not on subscription level.

upvoted 1 times

yana_b 1 year, 1 month ago

Solution provided by meinekarte is correct

upvoted 2 times

Govcomm 2 years, 1 month ago

Microsoft Defender for Azure SQL

upvoted 1 times

Ashutosh_9608 2 years, 11 months ago

https://docs.microsoft.com/en-us/azure/azure-sql/database/threat-detection-configure

upvoted 1 times

HOTSPOT -

Your company has an Azure subscription.

The company requires that all resource groups in the subscription have a tag named organization set to a value of Contoso.

You need to implement a policy to meet the tagging requirement.

How should you complete the policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
{
 "policyRule": {
   "if": {
     "allOf": [
       {
         "field": "type",
         "equals":
       },
       {
         "not": {
           "field": "tags['organization']",
           "equals": "Contoso"
         }
       }
     ]
   },
   "then": {
     "effect":
     "details": [
       {
         "field": "tags['organization']",
         "value": "Contoso"
       }
     ]
   }
 }
}
```

▼ "MicrosoftResources/deployments"
"MicrosoftResources/subscriptions"
"MicrosoftResources/subscriptions/resourceGroups"

▼ "Append",
"Deny",
"DeployIfNotExists",

Suggested Answer:

Answer Area

```
{
 "policyRule": {
   "if": {
     "allOf": [
       {
         "field": "type",
         "equals":
       },
       {
         "not": {
           "field": "tags['organization']",
           "equals": "Contoso"
         }
       }
     ]
   },
   "then": {
     "effect":
     "details": [
       {
         "field": "tags['organization']",
         "value": "Contoso"
       }
     ]
   }
 }
}
```

▼ "MicrosoftResources/deployments"
"MicrosoftResources/subscriptions"
"MicrosoftResources/subscriptions/resourceGroups"

▼ "Append",
"Deny",
"DeployIfNotExists",

Box 1: " Microsoft.Resources/subscriptions/resourceGroups"

Box 2: "Deny",

Sample - Enforce tag and its value on resource groups

```
},
"policyRule": {
"if": {
"allOf": [
{
"field": "type",
"equals": "Microsoft.Resources/subscriptions/resourceGroups"
},
{
"not": {
"field": "[concat('tags[',parameters('tagName'), ']')]",
"equals": "[parameters('tagValue')]"
}
}
]
},
"then": {
"effect": "deny"
}
}
}
}
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/samples/enforce-tag-on-resource-groups
```

Tos0 Highly Voted 4 years, 6 months ago

"The company requires that all resource groups in the subscription have a tag named organization set to a value of Contoso." - This means also the existing resource groups need to have a tag.

For that reason:

1. Microsoft.Resources/subscriptions/resourceGroups
2. Append

There is a pre-built policy in Azure for this, called: Append a tag and its value to resource groups

upvoted 131 times

MP270915 4 years, 5 months ago

Yes, it is Append, also because i wouldn't have that "details" propery below. That is used for Append, not for Deny.

https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects#append

upvoted 3 times

[Removed] 4 years, 5 months ago

No it is deny...because it is showing if Not contoso then deny the deployment....There is a not condition....if it was assignment then it would have been append

upvoted 7 times

hubeau 4 years, 5 months ago

If this resource groups hasn't a organization tag, we should append this tag onto this resource groups. So it should be append

upvoted 2 times

luango 4 years, 3 months ago

But append is intended for use with non-tag properties. So i think deny is the correct answer in this case.

upvoted 2 times

yemma 4 years, 3 months ago

Deny doesn't have any property, so the answer is Append and as Tos0 explained we have to correct the existing RG by appending the tag:

https://docs.microsoft.com/fr-fr/azure/governance/policy/concepts/effects#deny

upvoted 2 times

Morettimaxi 4 years, 2 months ago

Appends the specified tag with its value from the resource group when any resource which is missing this tag is created or updated. Does not modify the tags of resources created before this policy was applied until those resources are changed. New 'modify' effect policies are available that support remediation of tags on existing resources (see https://aka.ms/modifydoc

Append Does not modify the tags of resources created before this policy was applied until those resources are changed. New 'modify' effect policies are available that support remediation of tags on existing resources (see
upvoted 4 times

akp1000 2 years, 1 month ago
There is also a pre built policy named "Require a tag and its value on resource groups" It uses "Deny"
upvoted 1 times

prashantjoge 2 years, 5 months ago
When a policy definition using the append effect is run as part of an evaluation cycle, it doesn't make changes to resources that already exist. Instead, it marks any resource that meets the if condition as non-compliant.

https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects#append-evaluation
upvoted 1 times

prashantjoge 2 years, 5 months ago
For a Resource Manager mode, the deny effect doesn't have any additional properties for use in the then condition of the policy definition. Since additional properties are mentions, it has to be append
upvoted 2 times

Root_Access Highly Voted 4 years, 3 months ago
take my word back, if you are denying you dont need to specify tag name and value, but it is defined in the question, so it should be append. my bad.
upvoted 9 times

Chiboy 2 years, 4 months ago
Yes. If you review the resource Group and the Tag is not there, update the RG with the specified tag.
upvoted 1 times

e0da014 Most Recent 3 months ago
Final correct answer, verified
1. Microsoft.Resources/subscriptions/resourceGroups
2. Append
upvoted 2 times

chloaus 5 months, 1 week ago
2 is append.
https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effect-append
upvoted 1 times

zapi 5 months, 1 week ago
Microsoft.Resources/subscriptions/resourceGroups
DeployIfNotExists
That ensures that all resource groups are tagged
upvoted 1 times

hydrillo 11 months ago
For a deny policy the field and value properies wouldn't be neccessary and append is not for Tag as mentioned in other commends. Therefore I would go for "DeployIfNotExists". Any thoughts on this?
upvoted 1 times

gabo 11 months, 3 weeks ago
I think it's Append, because in the template, the effect is followed by the tag details, so that makes sense only if it's going to do an Append operation. If it's a deny, then what is the point of providing the tag details?
upvoted 1 times

Misterit 1 year, 1 month ago
looks correct, many suggest append or deployIfnotExist. but that should not work since there is no configuration in the example that points to an managed identity or service principal with permission to do this action
upvoted 2 times

Pukun 1 year, 3 months ago

```
{
"name": "Tagging policy",
"description": "Policy to require all resource groups to have a tag named organization set to a value of Contoso.",
"scope": {
"type": "Subscription"
},
"policyRule": {
"ruleType": "Tag",
"resourceType": "Microsoft.Resources/resourceGroups",
"tagSpecs": [
{
"tagName": "organization",
"tagValue": "Contoso"
}
],
"effect": "Deny"
}
}
```

upvoted 1 times

DGladiator 1 year, 4 months ago

GPT4

This policy will deny any resource group creation or update that does not include a tag named 'organization' with a value 'Contoso'.

upvoted 1 times

col2511kol 1 year, 5 months ago

In the policy definition, the "then" block defines the action that will be taken when the conditions specified in the "if" block are met. In this case, the action is "effect": "deny".

The "deny" effect means that if the conditions in the "if" block are met (i.e., the resource group does not have the required tag or the tag value is not "Contoso"), the policy will deny the creation or update of the resource group. As a result, the user attempting the action will receive an error message indicating that the operation is not allowed due to the policy.

In summary, the "then" block with the "effect": "deny" is used to enforce the policy by disallowing the creation or update of resource groups that do not meet the specified tagging requirements.

upvoted 1 times

col2511kol 1 year, 5 months ago

You can create and assign a custom Azure Policy to enforce the required tagging for all resource groups in the subscription. Here's an example of the policy definition:

```
{
"properties": {
"displayName": "Require organization tag",
"policyType": "Custom",
"mode": "Indexed",
"description": "Enforces the existence of the 'organization' tag with the value 'Contoso' on resource groups.",
"metadata": {
"version": "1.0.0",
"category": "Tags"
},
"parameters": {},
"policyRule": {
"if": {
"allof": [
{
"field": "type",
"equals": "Microsoft.Resources/subscriptions/resourceGroups"
},
{
```

"not": {
"field": "tags['organization']",
"equals": "Contoso"
}
}
]
},
"then": {
"effect": "deny"
}
}
}
}
upvoted 1 times

georgedevops_111 1 year, 8 months ago
The answer is append here is the reference:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F
6fd1-46fd-a676-f12d1d3a4c71
upvoted 4 times

Oluseun 1 year, 9 months ago
The given answer is correct. The question clearly states that the resourcegroups must have tags as a requirement. If they do not have tags it doesn't say that tags should be automatically added. It is thus logical that the resourcegroup creation should be denied.
upvoted 1 times

Atos 2 years ago
If you were going to use a deny policy then you wouldn't need the details.
It should be append.
upvoted 2 times

pdk88 2 years ago
I think the given answer is correct.

1. Microsoft.Resources/subscriptions/resourceGroups
2. Deny

According to this link (https://docs.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies#tags.) there are eight options with regards to assigning tags to resource groups. This particular case states the tag VALUE 'Contoso' is REQUIRED, hence we are looking for "Require a tag and its value on resource groups". When opening the link belonging to this tag, the policy says:

"displayName": "Require a tag and its value on resource groups",
"policyType": "BuiltIn",
"mode": "All",
"description": "Enforces a required tag and its value on resource groups."

[...]

"then": {
"effect": "deny"
upvoted 4 times

Darkeh 2 years, 1 month ago
Answer is append. Keyword is "requires." Append will set the value of what is specified in the details. I've done this before with hybrid benefit options on vm builds using a policy in the past.
upvoted 1 times

Question #34 *Topic 4*

You need to configure GitHub to use Azure Active Directory (Azure AD) for authentication.
What should you do first?

A. Create a conditional access policy in Azure AD.

B. Register GitHub in Azure AD.

C. Create an Azure Active Directory B2C (Azure AD B2C) tenant.

D. Modify the Security settings of the GitHub organization.

Suggested Answer: *B*
When you connect to a Git repository from your Git client for the first time, the credential manager prompts for credentials. Provide your Microsoft account or Azure
AD credentials.
Note: Git Credential Managers simplify authentication with your Azure Repos Git repositories. Credential managers let you use the same credentials that you use for the Azure DevOps Services web portal. Credential managers support multi-factor authentication through Microsoft account or Azure Active Directory (Azure
AD). Besides supporting multi-factor authentication with Azure Repos, credential managers also support two-factor authentication with GitHub repositories.
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/git/set-up-credential-managers

Community vote distribution

B (100%)

qrkon Highly Voted 3 years, 10 months ago
Given answer is correct.
Azure AD Enterprise Apps Market Place: Azure Active Directory> Enterprise Applications> New Application> Search and use Github
upvoted 20 times

kumardeb Highly Voted 3 years, 10 months ago
B. Register GitHub in Azure AD.
upvoted 5 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: B
Correct B
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: B
B is correct

From link given, you have to register for your credentials
upvoted 1 times

Govcomm 2 years, 1 month ago
App registration so register GitHub App is the correct answer.
upvoted 1 times

Eltooth 2 years, 4 months ago
Selected Answer: B
B is correct answer.
upvoted 1 times

UnknowMan 2 years, 4 months ago
Correct
upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: B

correct answer

upvoted 1 times

LieJ0n 2 years, 6 months ago

Selected Answer: B

Looks B to me

https://docs.github.com/en/github-ae@latest/admin/identity-and-access-management/configuring-authentication-and-provisioning-with-your-identity-provider/configuring-authentication-and-provisioning-for-your-enterprise-using-azure-ad

upvoted 1 times

Sumit4666 2 years, 8 months ago

B is correct.

https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/github-enterprise-cloud-enterprise-account-tutorial

upvoted 1 times

malikimran21 2 years, 9 months ago

this came in today exam Az-400 (Dec 2021)

upvoted 1 times

Dalias 3 years, 2 months ago

got this in 30 Jun 2021 exams. scored 800+ marks. B is correct

upvoted 5 times

nickc1 3 years, 2 months ago

So you got some wrong?

upvoted 2 times

Saintu 3 years, 1 month ago

You got alot wrong.

upvoted 2 times

Question #35 *Topic 4*

You have an Azure DevOps project named Project1 and an Azure subscription named Sub1.
You need to prevent releases from being deployed unless the releases comply with the Azure Policy rules assigned to Sub1.
What should you do in the release pipeline of Project1?

A. Add a deployment gate.

B. Modify the Deployment queue settings.

C. Configure a deployment trigger.

D. Create a pipeline variable.

Suggested Answer: *A*
You can check policy compliance with gates.
You can extend the approval process for the release by adding a gate. Gates allow you to configure automated calls to external services, where the results are used to approve or reject a deployment.
You can use gates to ensure that the release meets a wide range or criteria, without requiring user intervention.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/release/deploy-using-approvals

Community vote distribution
A (100%)

077dammy Highly Voted 3 years, 7 months ago
Deployment gate is correct
upvoted 17 times

vsvaid Most Recent 9 months ago
Selected Answer: A
Agree with A
upvoted 1 times

GirishGururani 1 year, 1 month ago
A. Add a deployment gate is correct.
Gates >> Check Azure Policy compliance
upvoted 1 times

flafernan 1 year, 1 month ago
Selected Answer: A
If you want to prevent a (release) from being deployed within Azure DevOps, following Azure Policies rules, it is necessary that within the pre-deployment conditions, in the option of GATEs enabled, “Check Policy Compliance” is added.
upvoted 1 times

zellck 1 year, 3 months ago
Selected Answer: A
A is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/tutorials/policy-devops-pipelines
upvoted 2 times

surensaluka 1 year, 7 months ago
Selected Answer: A
This question came today (2023-02-14)
upvoted 4 times

Jhest 2 years ago
I always think of Rocky Lee when I see this question.
upvoted 2 times

syu31svc 2 years, 1 month ago
Selected Answer: A

A is supported by given link and explanation

upvoted 2 times

Govcomm 2 years, 1 month ago

Add a deployment gate with the condition to control the quality.

upvoted 1 times

Eltooth 2 years, 3 months ago

Selected Answer: A

A is correct answer.

upvoted 2 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 1 times

AhmedHamdo 2 years, 5 months ago

Selected Answer: A

Correct

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: A

Correct

upvoted 1 times

Kolego 2 years, 11 months ago

Still relevant, got it today on the exam.

upvoted 2 times

SriLen 3 years, 7 months ago

Agree with given Answer , Deployment Gate

upvoted 4 times

Question #36 *Topic 4*

DRAG DROP -

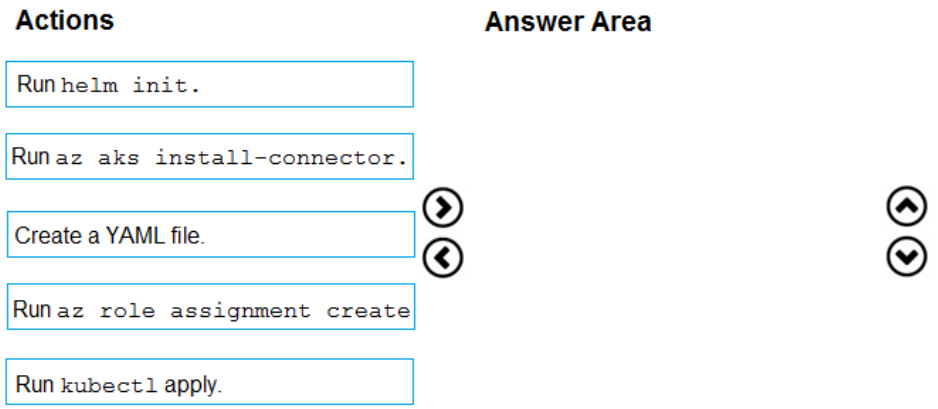
You have an Azure Kubernetes Service (AKS) implementation that is RBAC-enabled.

You plan to use Azure Container Instances as a hosted development environment to run containers in the AKS implementation.

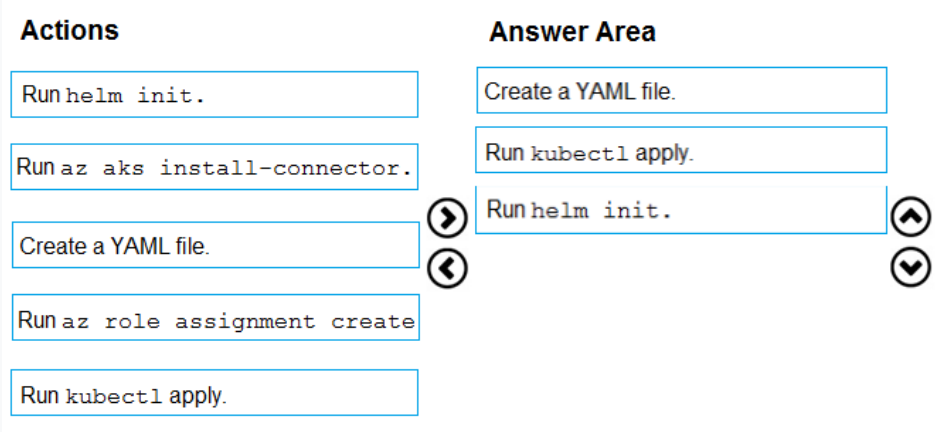
You need to configure Azure Container Instances as a hosted environment for running the containers in AKS.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Suggested Answer:



Step 1: Create a YAML file.

If your AKS cluster is RBAC-enabled, you must create a service account and role binding for use with Tiller. To create a service account and role binding, create a file named rbac-virtual-kubelet.yaml

Step 2: Run kubectl apply.

Apply the service account and binding with kubectl apply and specify your rbac-virtual-kubelet.yaml file.

Step 3: Run helm init.

Configure Helm to use the tiller service account:

helm init --service-account tiller

You can now continue to installing the Virtual Kubelet into your AKS cluster.

Reference:

https://docs.microsoft.com/en-us/azure/aks/virtual-kubelet

TosO Highly Voted 4 years, 5 months ago

With helm v3:

1. kubectl apply - to create the service principle for Tiller
2. helm init - to deploy Tiller in the kubernetes cluster
3. az aks install-connector - to install the connector

upvoted 48 times

TosO 4 years, 5 months ago

this is for v2, sorry

upvoted 5 times

nasa1515 3 years, 8 months ago

Is the answer correct?
upvoted 2 times

Saterial 3 years, 4 months ago
you need to take into context that this question was probably developed when Helm v2 was the deployment tool
upvoted 3 times

djhyfdgjk 7 months, 1 week ago
Where does the question ask anything about Helm ??
upvoted 2 times

thetrapt Highly Voted 4 years, 5 months ago
Answer is right. According to documentation, you create a YAML that defines service account and binding, then you apply that configuration and finally "deploy a basic Tiller into an AKS cluster". https://docs.microsoft.com/en-us/azure/aks/kubernetes-helm
upvoted 24 times

hubeau 4 years, 5 months ago
You're right:

1. Create a file named helm-rbac.yaml
2. kubectl apply -f helm-rbac.yaml
3. helm init --history-max 200 --service-account tiller...
4. $ helm install stable/nginx-ingress --set controlle....

upvoted 15 times

FeriAZ Most Recent 6 months, 1 week ago
Create a YAML file (rbac-virtual-kubelet.yaml):

Define a service account for the virtual kubelet.
Specify the necessary role bindings to grant the service account required permissions within the AKS cluster.
Run kubectl apply:

Apply the rbac-virtual-kubelet.yaml file using this command.
This creates the service account and assigns the role bindings, enabling the virtual kubelet to interact with the cluster resources.
Run helm init --service-account tiller:

This step becomes relevant only when using Helm with the virtual kubelet.
upvoted 2 times

varinder82 9 months, 3 weeks ago
Final Answer after going through all the comments
1) Run az role assignment create
2) Create a YAML file
3) Run kubectl apply

There is no az aks install-connector command
helm has nothing to do here
upvoted 10 times

yana_b 1 year, 1 month ago
1. run az role assignment create
2. create a yaml file
3. run kubectl -apply -f (i.e. file name to be applied) -> The kubectl apply command is a declarative way of deploying resources on a cluster using YAML manifest files

https://docs.microsoft.com/en-us/azure/aks/azure-ad-rbac
https://karthi-net.medium.com/kubernetes-tutorial-create-deployments-using-yaml-file-90ea901a2f74
https://www.geeksforgeeks.org/kubernetes-kubectl-create-and-kubectl-apply/
upvoted 7 times

renzoku 1 year, 2 months ago
I think
1.az aks install-connector

Install the Azure Container Instances Connector on your AKS cluster to enables the deployment of containers on Azure Container Instances.

2. Create YAML file
Called manifest file, describes the desired state of the pods or containers you want to deploy on Azure Container Instances within your AKS cluster.

3. kubectl apply
Used to deploy Kubernetes resources in AKS using an specific manifest file(YML or JSON)
e.g.
kubectl apply -f deployment.yaml
upvoted 6 times

adityagoel26 1 year, 5 months ago
To configure Azure Container Instances as a hosted environment for running containers in AKS, you should perform the following actions in sequence:

Run az aks install-connector: This installs the Azure Monitor for containers connector on the AKS cluster, which enables monitoring of container logs, metrics, and performance data from Azure Container Instances.

Create a YAML file: This file describes the container deployment and specifies the connection details for the Azure Monitor for containers connector.

Run kubectl apply: This deploys the container to AKS using the YAML file created in step 2.

Therefore, the correct sequence of actions is as follows:

B. Run az aks install-connector
C. Create a YAML file
E. Run kubectl apply

Note: Running helm init and az role assignment create are not necessary for configuring Azure Container Instances as a hosted environment for running containers in AKS.
upvoted 4 times

kay000001 1 year, 3 months ago
This is from GPT. Can you provide a link instead?
upvoted 3 times

Yatoom 1 year, 10 months ago
Tiller is no longer used in Helm, so this is probably an outdated question. However, if you want to know more about the integration between AKS and ACI, I suggest you to read this:

https://learn.microsoft.com/en-us/azure/architecture/solution-ideas/articles/scale-using-aks-with-aci
upvoted 4 times

kmaneith 1 year, 10 months ago
read this https://learn.microsoft.com/en-us/azure/aks/virtual-nodes-cli
upvoted 1 times

syu31svc 2 years, 1 month ago
I dont see what has helm got to do with this and there is no az aks install-connector command

https://docs.microsoft.com/en-us/azure/aks/azure-ad-rbac

1) Run az role assignment create
2) Create a YAML file
3) Run kubectl apply
upvoted 19 times

Pamban 1 year, 3 months ago
I think this is the best explanation and the link
upvoted 1 times

Govcomm 2 years, 1 month ago
It is RBAC enabled. So "az role assignment"
Create a YAML file
Kublctl apply to apply the YAML file
upvoted 6 times

Dileep75 2 years, 2 months ago
the answer is
Run az role assignment
create yaml file
kubectl apply
pls read the link provided in examtopic answer
upvoted 3 times

Eltooth 2 years, 3 months ago
Steps from MS Docs: https://docs.microsoft.com/en-us/azure/aks/azure-ad-rbac
1. az ad group create
2. az role assignment create command.
3. (az ad user create & az ad group member add) - optional
4. kubectl create
5. kubectl apply -f *.yaml

So answer is:
1. Run az role assignment create
2. Create YAML file
3. Run kubectl apply
upvoted 16 times

prashantjoge 2 years, 5 months ago
Helm init
Role assignment
install-connector
https://www.danielstechblog.io/deploying-kubernetes-aci-connector-aks-managed-kubernetes-azure/
upvoted 1 times

prashantjoge 2 years, 5 months ago
Sorry this is an old article, the connector works with helm2 . Use enable-addons instead
https://stackoverflow.com/questions/59968396/az-aks-install-connector-fails-name-uknow-parameter
upvoted 1 times

mountainking 2 years, 8 months ago
there two concepts for integrating with ACI in aks, virtual nodes vs virtual kubelet
for virtual kubelet - az aks install-connect
for setting up virtual nodes - I believe this what the question asks about
1) create service principle, role assignment
2) edit yaml
3) kubectl apply -f yaml

it's nothing to do with helm
upvoted 12 times

ixl2pass 2 years, 8 months ago
The question is about AKS with RBAC. So the correct answer is
a) az role assignment create
b) YAML file
c) kubectl apply
Reference: https://docs.microsoft.com/en-us/azure/aks/azure-ad-rbac
upvoted 13 times

rdemontis 2 years, 6 months ago
I think you are right. because we have to interact with a RBAC enabled AKS to use commands against AKS we need to create a role assgnoment

https://docs.microsoft.com/en-us/azure/aks/azure-ad-rbac

now to use ACI as host environment we need to use Virtual Nodes. So we can create the yaml file with the ACI container deployment and apply it.

https://docs.microsoft.com/en-us/azure/aks/virtual-nodes-portal
upvoted 3 times

prashantjoge 2 years, 5 months ago
This is the correct answer. has nothing to do with helm
upvoted 2 times

sdhfhsdorr 3 years ago
Based on my research this is correct also some answers point to same.
1. run az role assignment
2. Create YAML
3. Run Kubectl apply

Refer this https://cloud.netapp.com/blog/azure-cvo-blg-azure-kubernetes-service-tutorial-integrate-aks-with-aci
upvoted 6 times

[Removed] 2 years, 9 months ago
Am not sure about that i will go with role assignment, yaml, kubectl apply.
upvoted 3 times

erico 3 years, 2 months ago
First you can use the kubectl create command to create the Kubernetes cluster
Next you need to use the helm init command to start working with Helm
Next you can install the chart with the help of helm install command
upvoted 1 times

Question #37 *Topic 4*

You have an Azure DevOps project that contains a build pipeline. The build pipeline uses approximately 50 open source libraries.
You need to ensure that all the open source libraries comply with your company's licensing standards.
Which service should you use?

A. Ansible

B. Maven

C. WhiteSource Bolt

D. Helm

Suggested Answer: *C*
WhiteSource provides WhiteSource Bolt, a lightweight open source security and management solution developed specifically for integration with Azure DevOps and Azure DevOps Server.
Note: WhiteSource is the leader in continuous open source software security and compliance management. WhiteSource integrates into your build process, irrespective of your programming languages, build tools, or development environments. It works automatically, continuously, and silently in the background, checking the security, licensing, and quality of your open source components against WhiteSource constantly-updated definitive database of open source repositories.
Note: Blackduck would also be a good answer, but it is not an option here.
Reference:
https://www.azuredevopslabs.com/labs/vstsextend/whitesource/

Community vote distribution

C (100%)

gfdgdga 1 year, 8 months ago

Selected Answer: C

correct

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: C

Can only be C

Ansible, Maven and Helm are about automation

upvoted 2 times

Eltooth 2 years, 3 months ago

Selected Answer: C

C is correct answer.

upvoted 2 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 2 times

rdj17629 2 years, 4 months ago

Selected Answer: C

Correct imo

upvoted 3 times

Question #38 *Topic 4*

You are designing the security validation strategy for a project in Azure DevOps.
You need to identify package dependencies that have known security issues and can be resolved by an update.
What should you use?

A. Octopus Deploy

B. Jenkins

C. Gradle

D. SonarQube

Suggested Answer: *A*
Incorrect Answers:
B: Jenkins is a popular open-source automation server used to set up continuous integration and delivery (CI/CD) for your software projects.
D: SonarQube is a set of static analyzers that can be used to identify areas of improvement in your code. It allows you to analyze the technical debt in your project and keep track of it in the future.
Reference:
https://octopus.com/docs/packaging-applications

Community vote distribution

D (96%) 4%

dollarpo7 Highly Voted 3 years, 10 months ago
Should be Sonarqube
upvoted 54 times

Pavlo 1 year, 3 months ago
A. Octopus Deploy
B. Jenkins
C. Gradle
D. SonarQube<<<<<<<<<<<<<<<<<<<<<<<<
upvoted 1 times

Ahmed0 Highly Voted 3 years, 8 months ago
WTF who selected this answer ?
upvoted 30 times

larrymm 2 years, 1 month ago
At this point I just feel the do this on purpose cos wth
upvoted 2 times

hbergun 3 years, 6 months ago
Maybe Math.Random
upvoted 42 times

jojom19980 3 years, 2 months ago
maybe, hh, you are right
upvoted 2 times

GPRai Most Recent 2 months, 3 weeks ago
Selected Answer: D
SonarQube
upvoted 1 times

UrbanRellik 4 months ago
Selected Answer: D
I'd rather not explain myself. The answer is D, SonarQube.
upvoted 1 times

Ghauri07 11 months, 3 weeks ago

Selected Answer: A

Because Sonarqube did the code analysis

upvoted 1 times

yana_b 1 year, 1 month ago

Selected Answer: D

SonarQube

upvoted 1 times

resonant 1 year, 2 months ago

You can use SonarQube but arent you supposed to use MendBolt?

upvoted 1 times

klayytech 1 year, 6 months ago

Selected Answer: D

Octopus Deploy is a tool to manage releases and deploy the release it-self to the destination host, the Azure DevOps substitute is "Release PipeLine"

SonarQube is for sure the correct answer

upvoted 6 times

syu31svc 2 years, 1 month ago

Selected Answer: D

This is D for sure

upvoted 3 times

Govcomm 2 years, 1 month ago

SonarQube

upvoted 1 times

Eltooth 2 years, 4 months ago

Selected Answer: D

D is correct answer.

upvoted 2 times

UnknowMan 2 years, 4 months ago

Selected Answer: D

SonarQube can check for security licence

upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: D

I think correct answer id D.

There is a plugin (dependency-check) for SonarQube that do exactly what it is required by the questions. Not a scan of the dependencies but a control based on known security issues

https://github.com/dependency-check/dependency-check-sonar-plugin

upvoted 6 times

kennynelcon 2 years, 1 month ago

Thank You

upvoted 1 times

Optimist_Indian 2 years, 7 months ago

Got this question in Feb-2022 exam (scored 910+). Answer : SonarQube.

upvoted 5 times

durel 2 years, 7 months ago

Selected Answer: D

should be D

upvoted 1 times

Art3 2 years, 8 months ago

Selected Answer: D

Obviously D.

upvoted 1 times

Pankaj78 2 years, 9 months ago

Selected Answer: D

Octopus deploy is solely responsible for automated deployment management

upvoted 1 times

Question #39 *Topic 4*

You administer an Azure DevOps project that includes package feeds.
You need to ensure that developers can unlist and deprecate packages. The solution must use the principle of least privilege.
Which access level should you grant to the developers?

A. Collaborator

B. Contributor

C. Owner

Suggested Answer: *B*
Feeds have four levels of access: Owners, Contributors, Collaborators, and Readers. Owners can add any type of identity-individuals, teams, and groups-to any access level.

Permission	Reader	Collaborator	Contributor	Owner
List and restore/install packages	✓	✓	✓	✓
Save packages from upstream sources		✓	✓	✓
Push packages			✓	✓
Unlist/deprecate packages			✓	✓
Promote a package to a view			✓	✓
Delete/unpublish package				✓
Edit feed permissions				✓

Reference:
https://docs.microsoft.com/en-us/azure/devops/artifacts/feeds/feed-permissions

Community vote distribution
B (100%)

Dalias Highly Voted 3 years, 2 months ago
got this in 30 Jun 2021 exams. scored 800+ marks. THis is correct!
upvoted 15 times

SteveChai Highly Voted 3 years, 4 months ago
VERIFIED - given answer is correct
upvoted 8 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: B
correct
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: B
B is the answer and 100% supported by link given
upvoted 1 times

Govcomm 2 years, 1 month ago
Contributor: unlist the package
upvoted 1 times

Eltooth 2 years, 3 months ago
Selected Answer: B

B is correct answer.

Contributor.

upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: B

correct answer as demonstrated in the document attached

upvoted 2 times

Optimist_Indian 2 years, 7 months ago

Got this question in Feb-2022 exam (scored 910+). Given answer is correct.

upvoted 1 times

subrata83 2 years, 11 months ago

Got this in the Az-400 exam(Sep 27 2021)

upvoted 1 times

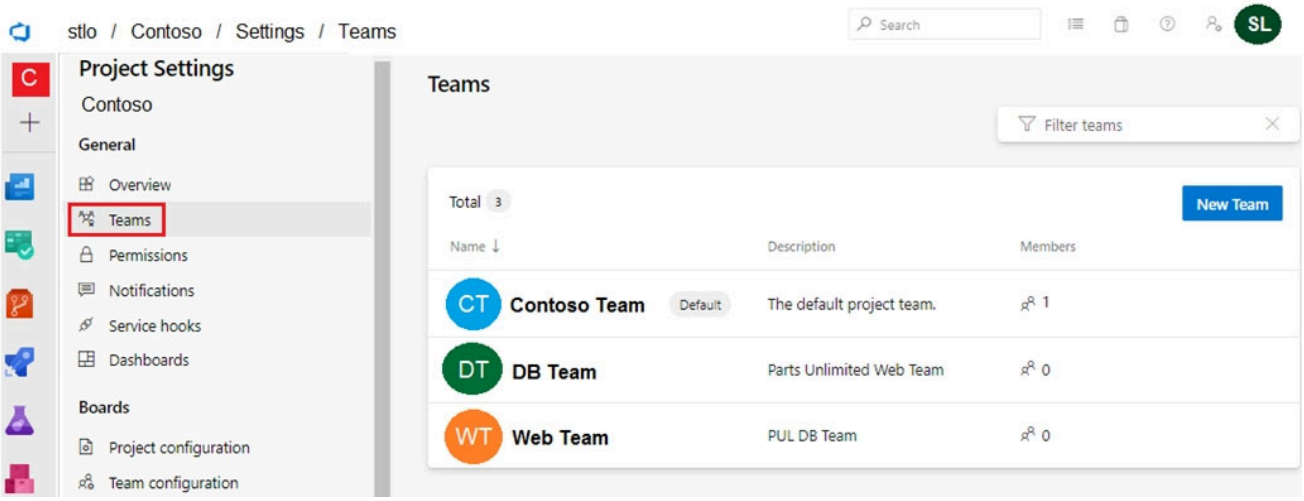
V_Ramon 3 years, 1 month ago

this question came out today, July 28, 2021

upvoted 2 times

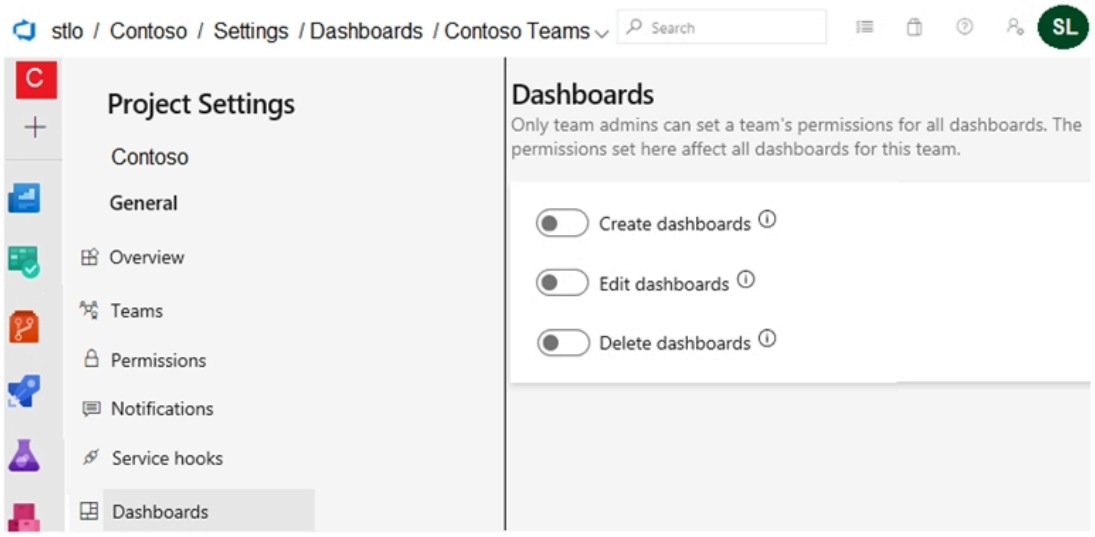
HOTSPOT -

You have a project in Azure DevOps that has three teams as shown in the Teams exhibit. (Click the Teams tab.)



You create a new dashboard named Dash1.

You configure the dashboard permissions for the Contoso project as shown in the Permissions exhibit. (Click the Permissions tab.)



All other permissions have the default values set.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

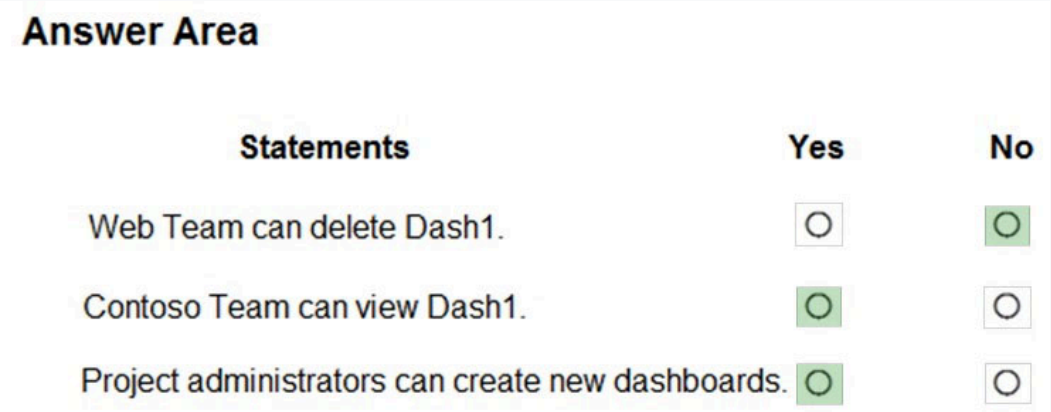
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Web Team can delete Dash1.	○	○
Contoso Team can view Dash1.	○	○
Project administrators can create new dashboards.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
Web Team can delete Dash1.	○	○
Contoso Team can view Dash1.	○	○
Project administrators can create new dashboards.	○	○

Reference:
https://docs.microsoft.com/en-us/azure/devops/report/dashboards/charts-dashboard-permissions-access

sheva370 Highly Voted 3 years, 1 month ago

The given answer is correct.

Box 1: No - According to the configuration in the second screenshot, Delete dashboards permission is disabled.
Box 2: Yes - Everyone can view a dashboard.
Box 3: Yes - Only project administrators can manage dashboards.
upvoted 19 times

giuliohome 2 years ago

The explanation is wrong: the second screenshot refers to Contoso Team, not to Web Team, the first answer is rather "No" because by default the deletion is not enabled ...
upvoted 10 times

armvch 1 year, 6 months ago

but why does the second screenshot has "Contoso Teams" not "Contoso Team" then?
upvoted 1 times

vasonic Highly Voted 3 years, 5 months ago

I think answer is correct:
"By default, all team members have permissions to create and edit dashboards for their teams."
Link: https://docs.microsoft.com/en-us/azure/devops/report/dashboards/dashboard-permissions?view=azure-devops
upvoted 13 times

resonant Most Recent 1 year ago

This question was on my exam on September 12, 2023. Choosed the following:
1- No
2- Yes
3- Yes
Passed with 877. I also submitted feedback pointing out that you can't really see the permissions assigned to each team.
upvoted 7 times

yana_b 1 year, 1 month ago

For me the answer looks correct.
upvoted 1 times

Rams_84zO6n 1 year, 6 months ago

No, Yes, Yes
Web team can delete dash1 - no (Contoso project permissions tab)
Contoso team can view dash1 - Yes (default view permission granted for all roles in team)
Project administrators can create new dashboards - Yes (contoso project permission tab denies permission, Project Admin role default permission allows add project dashboard)
Note: Dashbaord permissions set at project level overrides dashboard permissions set at team level
upvoted 2 times

xRiot007 1 year, 2 months ago

Answers are good, explanation is wrong.
No - by default, DevOps teams cannot delete dashboards, Contoso team included. It has nothing to do with the opened tab.

Yes - by default DevOps teams can view dashboards. There is nowhere in Contoso's tab a denial of that.
Yes - Project admins can add dashboards.
upvoted 1 times

syu31svc 2 years, 1 month ago
https://docs.microsoft.com/en-us/azure/devops/organizations/security/permissions-access?view=azure-devops

"By default, the Project Collection Build Service is a Contributor and your project team is a Reader"

Given answer is correct
upvoted 2 times

Govcomm 2 years, 1 month ago
No
Yes
Yes
upvoted 1 times

rdemontis 2 years, 5 months ago
For me the answer is correct
upvoted 3 times

malikimran21 2 years, 9 months ago
this came in today exam Az-400
upvoted 3 times

SuperPetey 3 years, 3 months ago
Nice Easter egg for The Unicorn Project by the MSFT devOps team. Like this comment if you see it.
upvoted 4 times

agustinleone 3 years, 2 months ago
no :) but comment content is too short so here i am
upvoted 2 times

Question #41 *Topic 4*

Your company is concerned that when developers introduce open source libraries, it creates licensing compliance issues.
You need to add an automated process to the build pipeline to detect when common open source libraries are added to the code base.
What should you use?

A. Microsoft Visual SourceSafe

B. Code Style

C. Black Duck

D. Jenkins

Suggested Answer: *C*
Secure and Manage Open Source Software
Black Duck helps organizations identify and mitigate open source security, license compliance and code-quality risks across application and container portfolios.
Black Duck Hub and its plugin for Team Foundation Server (TFS) allows you to automatically find and fix open source security vulnerabilities during the build process, so you can proactively manage risk. The integration allows you to receive alerts and fail builds when any Black Duck Hub policy violations are met.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
➪ Black Duck
➪ WhiteSource Bolt
Other incorrect answer options you may see on the exam include the following:
➪ OWASP ZAP
➪ PDM
➪ SourceGear

SourceGear Vault -
▪
Reference:
https://marketplace.visualstudio.com/items?itemName=black-duck-software.hub-tfs

Community vote distribution
C (100%)

Eltooth Highly Voted 2 years, 4 months ago
Selected Answer: C
C is correct answer.

FYI - there will be an update to exam content in June 2022 and all 3rd party questions will be removed.
upvoted 7 times

dang12394 Most Recent 2 months, 1 week ago
Selected Answer: C
quack quack
upvoted 2 times

zellck 1 year, 3 months ago
Selected Answer: C
C is the answer.

https://marketplace.visualstudio.com/items?itemName=black-duck-software.detect-for-tfs
The Black Duck by Synopsys plugin for TFS and Azure DevOps allows automatic identification of open source security vulnerabilities during your application build process. The integration allows you to enforce policies configured in Black Duck to receive alerts and fail builds when policy violations are met.
upvoted 2 times

zellck 1 year, 3 months ago

Black Duck by Synopsys helps organizations identify and manage open source security, license compliance and operational risks across applications and containers. Black Duck is powered by the world's largest open source KnowledgeBase™, which containins information from over 13,000 unique sources, includes support for over 80 programming languages, provides timely and enhanced vulnerability information, and is backed by a dedicated team of open source and security experts. The KnowledgeBase™, combined with the broadest support for platforms, languages and integrations, is why 2,000 organizations worldwide rely on Black Duck to secure and manage open source.
upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: C

"Overview
Black Duck Hub and its plugin for Team Foundation Server (TFS) allows you to automatically find and fix open source security vulnerabilities during the build process, so you can proactively manage risk. The integration allows you to receive alerts and fail builds when any Black Duck Hub policy violations are met."

Link supports C as the answer
upvoted 3 times

Govcomm 2 years, 1 month ago

Blackduck
upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct
upvoted 2 times

Question #42 *Topic 4*

DRAG DROP -

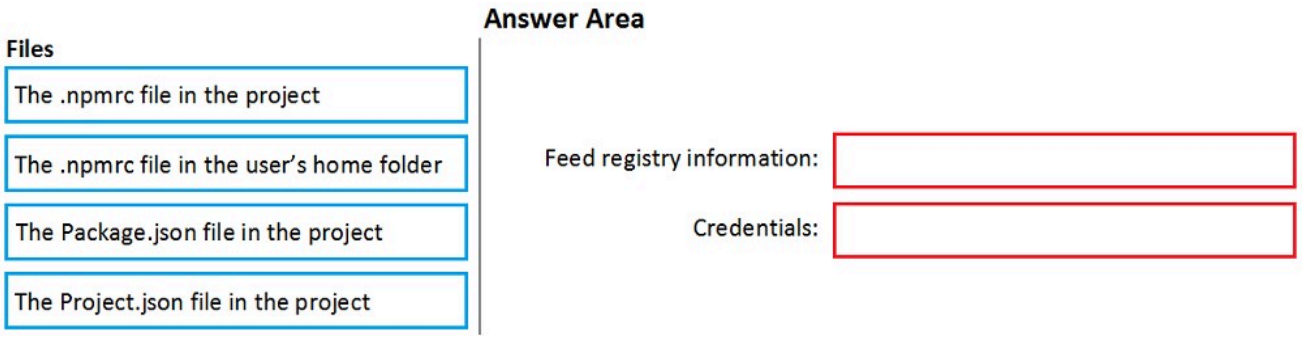
You are implementing a package management solution for a Node.js application by using Azure Artifacts.

You need to configure the development environment to connect to the package repository. The solution must minimize the likelihood that credentials will be leaked.

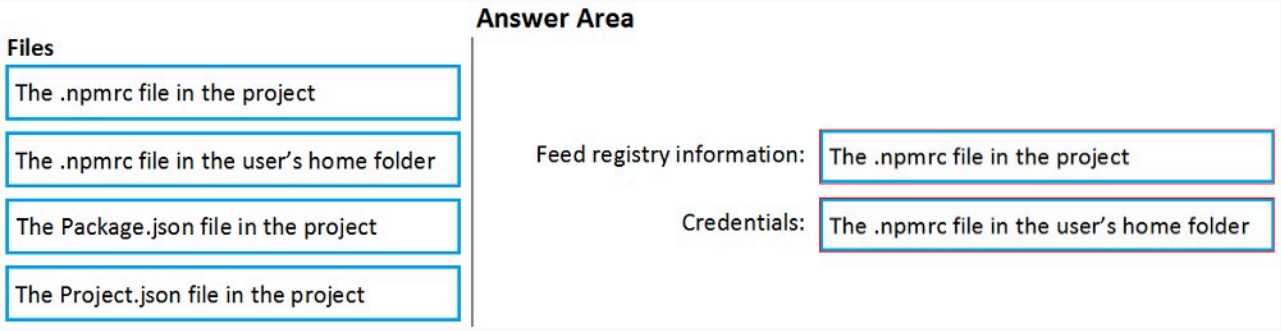
Which file should you use to configure each connection? To answer, drag the appropriate files to the correct connections. Each file may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested Answer:



All Azure Artifacts feeds require authentication, so you'll need to store credentials for the feed before you can install or publish packages. npm uses .npmrc configuration files to store feed URLs and credentials. Azure DevOps Services recommends using two .npmrc files.

Feed registry information: The .npmrc file in the project

One .npmrc should live at the root of your git repo adjacent to your project's package.json. It should contain a "registry" line for your feed and it should not contain credentials since it will be checked into git.

Credentials: The .npmrc file in the user's home folder

On your development machine, you will also have a .npmrc in $home for Linux or Mac systems or $env.HOME for win systems. This .npmrc should contain credentials for all of the registries that you need to connect to. The NPM client will look at your project's .npmrc, discover the registry, and fetch matching credentials from $home/.npmrc or $env.HOME/.npmrc.

Reference:

https://docs.microsoft.com/en-us/azure/devops/artifacts/npm/npmrc?view=azure-devops&tabs=windows

enowman Highly Voted 4 years ago

The answer on examtopics is correct.

https://docs.microsoft.com/en-us/azure/devops/artifacts/get-started-npm?view=azure-devops&tabs=windows#set-up-authentication-on-your-development-machine

upvoted 31 times

PM2 4 years ago

Agree

.npmrc should contain credentials for all of the registries that you need to connect to. The NPM client will look at your project's .npmrc, discover the registry, and fetch matching credentials from $home/.npmrc or $env.HOME/.npmrc.

upvoted 9 times

27close Highly Voted 3 years, 10 months ago

The NPM client will look at your project's .npmrc, discover the registry, and fetch matching credentials from $home/.npmrc or $env.HOME/.npmrc.
so credential -home folder
upvoted 7 times

zellck Most Recent 1 year, 3 months ago
1. .npmrc file in the project
2. .npmrc file in user's home folder

https://learn.microsoft.com/en-us/azure/devops/artifacts/npm/npmrc
Azure Artifacts enables you to publish various package types to your feeds and install packages from both feeds and public registries like npmjs.com. Before we can authenticate with Azure Artifacts, we need to configure our .npmrc file, which stores the feed URLs and credentials that Npm uses. This file can be used to customize the behavior of the Npm client, such as setting up proxies, specifying default package locations, or configuring private package feeds. The .npmrc file is located in the user's home directory and can also be created at the project level to override the default settings. By editing the .npmrc file, users can customize their Npm experience and make it more tailored to their needs.
upvoted 2 times

meoukg 1 year, 10 months ago
I saw this question in my exam yesterday
upvoted 4 times

syu31svc 2 years, 1 month ago
Given answer and link are correct
upvoted 2 times

tjeerd 2 years, 1 month ago
On exam 20220727. Given answer is correct.
upvoted 3 times

Govcomm 2 years, 1 month ago
1. Project
2. User home directory
upvoted 1 times

Cheehp 2 years, 5 months ago
Selected during exam.
The.npmrc file in the project
The .npmrc file in the user's home folder
upvoted 2 times

rdemontis 2 years, 5 months ago
correct answer
upvoted 1 times

dr_maq 4 years, 1 month ago
Field registry information will be saved in project.json file
The first answer is project.json
upvoted 2 times

Beer_Enjoyer 4 years, 1 month ago
https://docs.microsoft.com/en-us/azure/devops/artifacts/get-started-npm?view=azure-devops&tabs=windows#set-up-authentication-on-your-development-machine

So .npmrc is right
upvoted 6 times

Question #43 *Topic 4*

HOTSPOT -

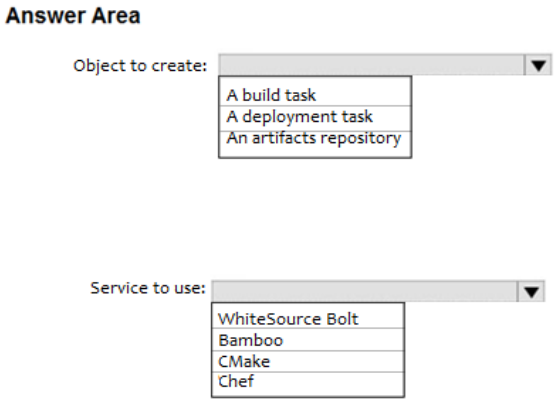
You have an Azure DevOps project that contains a build pipeline. The build pipeline uses approximately 50 open source libraries.

You need to ensure that the project can be scanned for known security vulnerabilities in the open source libraries.

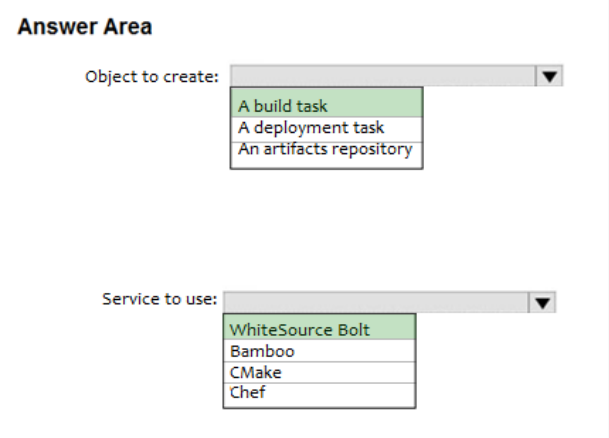
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:



Box 1: A Build task -

Trigger a build -

You have a Java code provisioned by the Azure DevOps demo generator. You will use WhiteSource Bolt extension to check the vulnerable components present in this code.

1. Go to Builds section under Pipelines tab, select the build definition WhiteSourceBolt and click on Queue to trigger a build.
2. To view the build in progress status, click on ellipsis and select View build results.

Box 2: WhiteSource Bolt -

WhiteSource is the leader in continuous open source software security and compliance management. WhiteSource integrates into your build process, irrespective of your programming languages, build tools, or development environments. It works automatically, continuously, and silently in the background, checking the security, licensing, and quality of your open source components against WhiteSource constantly-updated definitive database of open source repositories.

Reference:

https://www.azuredevopslabs.com/labs/vstsextend/whitesource/

PM2 Highly Voted 4 years ago

Correct verified

upvoted 36 times

Miles19 3 years, 5 months ago

Yes sure

upvoted 5 times

PDR Highly Voted 1 year, 2 months ago
correct , although just to add a note that Whitesource Bolt is now Mend Bolt , in case a similar question arises in exam with new name
upvoted 12 times

xda Most Recent 7 months, 2 weeks ago
January2024: Had the question, but with "Mend Bolt" as answer instead of WhiteSource. WihteSource was not avaiable to choose.
upvoted 4 times

WH16 1 year ago
On exam 2023-09-06, selected
1. Build task
2. WhiteSource Bolt
Answer is correct.
upvoted 7 times

zellck 1 year, 3 months ago
1. Build task
2. WhiteSource Bolt

https://marketplace.visualstudio.com/items?itemName=whitesource.whitesource
WhiteSource integrates with your CI servers, build tools and repositories to detect all open source components in your software, without ever scanning your code. It provides you with real-time alerts on vulnerable or problematic components, generates comprehensive up-to-date reports in one-click and enables you to streamline your entire open source management process with automated policies.
upvoted 3 times

syu31svc 2 years, 1 month ago
Given answer is correct
upvoted 2 times

tjeerd 2 years, 1 month ago
On exam 20220727.
Answer is correct.
upvoted 1 times

Govcomm 2 years, 1 month ago
Build pipeline
WhiteSource Bolt
upvoted 1 times

Eltooth 2 years, 3 months ago
A build task
WhiteSource Bolt
upvoted 3 times

UnknowMan 2 years, 4 months ago
Correct
upvoted 1 times

rdemontis 2 years, 6 months ago
correct
upvoted 1 times

lugospod 2 years, 7 months ago
Got this January 2022. Correct. (100% on that part)
upvoted 4 times

jojom19980 3 years, 2 months ago
Correct answer
upvoted 2 times

Question #44 *Topic 4*

You have an Azure DevOps project that contains a build pipeline. The build pipeline uses approximately 50 open source libraries.
You need to ensure that all the open source libraries comply with your company's licensing standards.
Which service should you use?

A. NuGet

B. Maven

C. Black Duck

D. Helm

Suggested Answer: *C*
Secure and Manage Open Source Software
Black Duck helps organizations identify and mitigate open source security, license compliance and code-quality risks across application and container portfolios.
Black Duck Hub and its plugin for Team Foundation Server (TFS) allows you to automatically find and fix open source security vulnerabilities during the build process, so you can proactively manage risk. The integration allows you to receive alerts and fail builds when any Black Duck Hub policy violations are met.
Note: WhiteSource would also be a good answer, but it is not an option here.
Reference:
https://marketplace.visualstudio.com/items?itemName=black-duck-software.hub-tfs

Community vote distribution

C (100%)

Geetesh05 Highly Voted 2 years, 1 month ago
general keywords for these questions

open libraries + scan = whitesource bolt
open libraries + license = black duck
upvoted 20 times

resonant 1 year, 2 months ago
I think you can use whitesource bolt to check licenses. Whitesource bolt is not included among the available answers anyways...
upvoted 1 times

zellck Most Recent 1 year, 3 months ago
Selected Answer: C
C is the answer.

https://marketplace.visualstudio.com/items?itemName=black-duck-software.detect-for-tfs
Black Duck by Synopsys helps organizations identify and manage open source security, license compliance and operational risks across applications and containers. Black Duck is powered by the world's largest open source KnowledgeBase™, which containins information from over 13,000 unique sources, includes support for over 80 programming languages, provides timely and enhanced vulnerability information, and is backed by a dedicated team of open source and security experts. The KnowledgeBase™, combined with the broadest support for platforms, languages and integrations, is why 2,000 organizations worldwide rely on Black Duck to secure and manage open source.
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: C
100% is C
upvoted 1 times

kennynelcon 2 years, 1 month ago
Selected Answer: C
correct
upvoted 1 times

Govcomm 2 years, 1 month ago

Blackduck

upvoted 1 times

Eltooth 2 years, 3 months ago

Selected Answer: C

C is correct answer.

Black Duck

upvoted 2 times

jpvdham 2 years, 4 months ago

Answer is correct.

upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 1 times

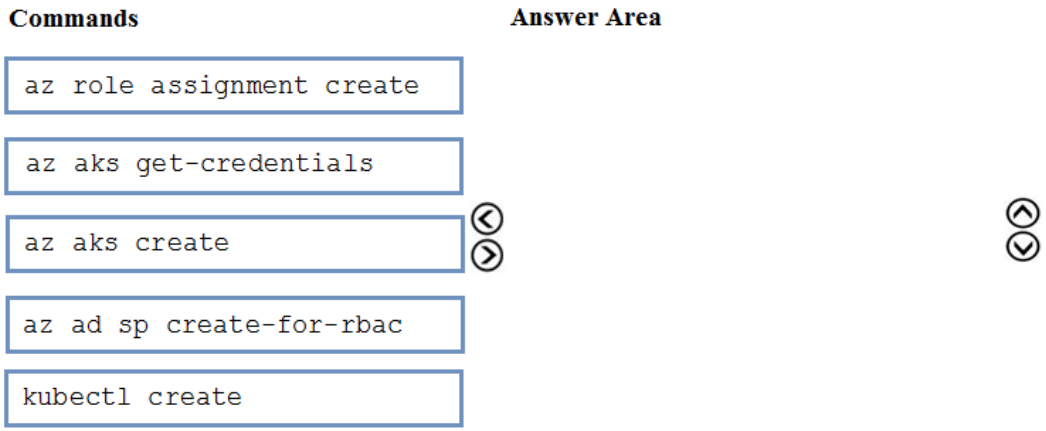
DRAG DROP -

You plan to use Azure Kubernetes Service (AKS) to host containers deployed from images hosted in a Docker Trusted Registry.

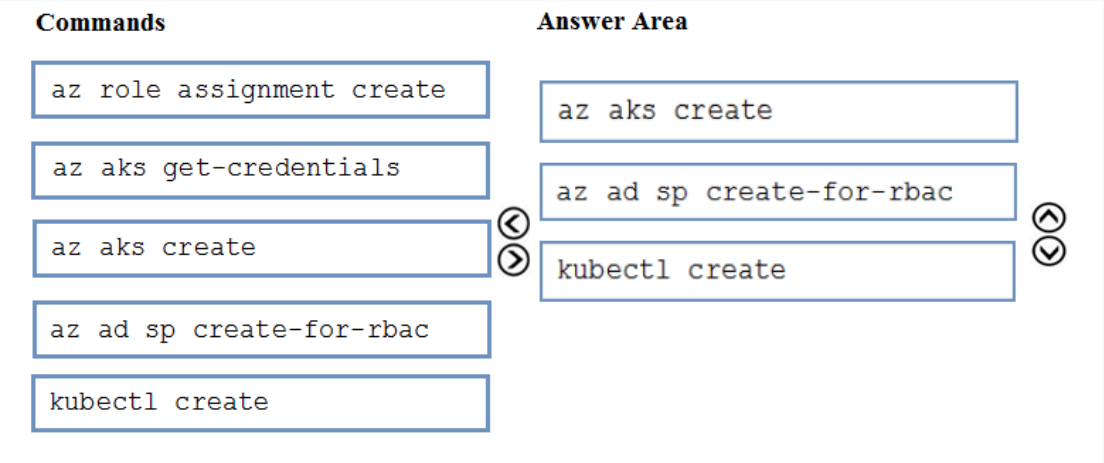
You need to recommend a solution for provisioning and connecting to AKS. The solution must ensure that AKS is RBAC-enabled and uses a custom service principal.

Which three commands should you recommend be run in sequence? To answer, move the appropriate commands from the list of commands to the answer area and arrange them in the correct order.

Select and Place:



Suggested Answer:



Step 1 : az acr create -

An Azure Container Registry (ACR) can also be created using the new Azure CLI. az acr create

--name <REGISTRY_NAME>

--resource-group <RESOURCE_GROUP_NAME>

--sku Basic

Step 2: az ad sp create-for-rbac

Once the ACR has been provisioned, you can either enable administrative access (which is okay for testing) or you create a Service Principal (sp) which will provide a client_id and a client_secret. az ad sp create-for-rbac

--scopes

/subscriptions/<SUBSCRIPTION_ID>/resourcegroups/<RG_NAME>/providers/Microsoft.ContainerRegistry/registries/<REGISTRY_NAME>

--role Contributor

--name <SERVICE_PRINCIPAL_NAME>

Step 3: kubectl create -

Create a new Kubernetes Secret.

kubectl create secret docker-registry <SECRET_NAME>

--docker-server <REGISTRY_NAME>.azurecr.io

--docker-email <YOUR_MAIL>

--docker-username=<SERVICE_PRINCIPAL_ID>

--docker-password <YOUR_PASSWORD>

Reference:
https://thorsten-hans.com/how-to-use-private-azure-container-registry-with-kubernetes

TosO Highly Voted 4 years, 6 months ago
1. az ad sp create-for-rbac - create the service principle
2. az aks create - create the aks with the service principle
3. az role assignment - delegate access to other resources
upvoted 176 times

Duleep 4 years, 1 month ago
"The solution must ensure that AKS is RBAC-enabled" So it need "kubectl create"
upvoted 4 times

s9p3r7 3 years ago
the recommended solution should be for PROVISIONING and CONNECTING
upvoted 5 times

rdemontis 2 years, 5 months ago
agree with you!
https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal
upvoted 5 times

canbe20 3 years, 8 months ago
Moreover az ad sp create-for-rbac can create the role assignment too, so you don't need to repeat it using az role assignment but run kubectl create
upvoted 7 times

silverdeath Highly Voted 4 years, 5 months ago
1- az aks create
2- az ad sp create-for-rbac
3- az role assignment create
https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal
upvoted 39 times

silverdeath 4 years, 5 months ago
typo swap 1 and 2
upvoted 26 times

rdemontis 2 years, 6 months ago
Agree with you. thanks for sharing the document
upvoted 4 times

rdemontis 2 years, 5 months ago
Looking better at the document you shared I think it is more correct to create the service principal first. So it would become:
1. az ad sp create-for-rbac
2. az aks create
3. az role assignment
upvoted 9 times

VinayDev 3 years, 3 months ago
Agree with Silverdeath..
upvoted 3 times

ozbonny Most Recent 6 months, 3 weeks ago
az ad sp create-for-rbac
az aks create
az role assignment create
upvoted 3 times

varinder82 9 months, 3 weeks ago
Final answer after going through all the comments
1. az ad sp create-for-rbac - create the service principle
2. az aks create - create the aks with the service principle
3. az role assignment - delegate access to other resources

upvoted 9 times

yana_b 10 months, 3 weeks ago

https://learn.microsoft.com/en-us/azure/aks/kubernetes-service-principal?tabs=azure-cli

1. az ad sp create-for-rbac
2. az aks create
3. az role assignment

upvoted 3 times

CirusD 11 months, 3 weeks ago

az ad sp create-for-rbac
az aks create
az aks get-credentials

upvoted 2 times

yana_b 1 year, 1 month ago

https://learn.microsoft.com/en-us/azure/aks/kubernetes-service-principal?tabs=azure-cli
This link evidences that the answer provided by TosO is still valid.

upvoted 2 times

zellck 1 year, 3 months ago

1. az ad sp create-for-rbac
2. az aks create
3. az role assignment create

https://learn.microsoft.com/en-us/azure/aks/kubernetes-service-principal?tabs=azure-cli#manually-create-a-service-principal
To manually create a service principal with the Azure CLI, use the az ad sp create-for-rbac command.

https://learn.microsoft.com/en-us/azure/aks/kubernetes-service-principal?tabs=azure-cli#specify-a-service-principal-for-an-aks-cluster
To use an existing service principal when you create an AKS cluster using the az aks create command, use the --service-principal and --client-secret parameters to specify the appId and password from the output of the az ad sp create-for-rbac command:

https://learn.microsoft.com/en-us/azure/aks/kubernetes-service-principal?tabs=azure-cli#delegate-access-to-other-azure-resources
To delegate permissions, create a role assignment using the az role assignment create command. Assign the appId to a particular scope, such as a resource group or virtual network resource.

upvoted 9 times

Pukun 1 year, 3 months ago

1. az ad sp create-for-rbac
2. az aks create
3. az aks get-credentials

--Use the az ad sp create-for-rbac command to create a custom service principal in Azure Active Directory (AD) with the necessary permissions to interact with AKS. This command will generate the required credentials for the service principal.
--Use the az aks create command to create the AKS cluster. This command will provision the AKS cluster with the specified configuration, including RBAC settings. You can specify the custom service principal created in the previous step using the --service-principal and --client-secret parameters.
--Use the az aks get-credentials command to retrieve the necessary credentials and configuration to connect to the AKS cluster. This command will download and merge the cluster's kubeconfig file with your local kubeconfig, allowing you to interact with the cluster using kubectl.

upvoted 4 times

Fal991l 1 year, 5 months ago

here are the three recommended commands in the correct order:

az ad sp create-for-rbac to create a new service principal with a custom name and assign it the Contributor role on your Azure subscription.
az aks create to create an AKS cluster and specify the service principal and RBAC enabled.
az aks get-credentials to get the Kubernetes configuration files for the AKS cluster and merge them into your local configuration.
Explanation:

The az ad sp create-for-rbac command creates a new service principal with a custom name and assigns it the Contributor role on your Azure subscription. This command returns the appId, password, and tenant values that are needed to configure AKS.
The az aks create command creates an AKS cluster, specifies the custom service principal, and enables RBAC. This command also returns the

Kubernetes configuration files that are needed to connect to the cluster.
The az aks get-credentials command gets the Kubernetes configuration files for the AKS cluster and merges them into your local configuration.
This command enables you to connect to the AKS cluster using kubectl.
upvoted 3 times

Fal991l 1 year, 5 months ago
from GPT
upvoted 1 times

gregigitty 1 year, 7 months ago
Custom principal -> az ad sp create-for-RBAC. ('az aks create' can create a system managed identity automatically but not a custom principal).
Create AKS cluster -> az aks create
Connect to the AKS cluster -> az aks get-credentials
"Configure kubectl to connect to your Kubernetes cluster using the az aks get-credentials command."
https://learn.microsoft.com/en-us/azure/aks/learn/quick-kubernetes-deploy-cli#connect-to-the-cluster

"az role assignment create" - In my opinion this is not needed as the cluster is "RBAC-Enabled", just not assigned any roles.
upvoted 3 times

ParkXD 1 year, 6 months ago
same with the answer from chatGPT:
1. Create a service principal:
2. Create an AKS cluster:
3.Connect to the AKS cluster
upvoted 1 times

ecpcloud 1 year, 9 months ago
To me all of this seems confusing, as everyone kinda leans towards the most common answer. But it's important to note the "az ad sp create-for-rbac" command can directly specify the role assignment and scope, so that'd eliminate the need for "az role assignment" one.

Then, given the question is asking to PROVISION and CONNECT to the cluster, to me the sequence should be:
1. az ad sp create-for-rbac - create the service principal & also assign it the role (Contributor)
2. az aks create - create the aks specifying a custom service principal, i.e. the one from above, so the aks will already have the role
3. az aks get-credentials - specify the rg and cluster-name from above, to get the credentials to connect to it after you've created it

But we all know how Microsoft can be in these situations, my answer might be correct but also overthought, while MS just wanted us to do a few simple initial steps... I genuinely don't know
upvoted 9 times

Atos 2 years ago
Looks like the article has been updated as it clearly states:
1. az ad sp create-for-rbac
2. az aks create
3. az role assignment
upvoted 8 times

shafqat 2 years, 1 month ago
3. az aks get-credentials --resource-group <group name> -name <cluster-name> : this is used for connecting from your machine to aks cluster you created in step 2.
upvoted 2 times

matelin 1 year, 7 months ago
Agree. In my opinion the answer is:
1. az ad sp create-for-rbac
2. az aks create
3. az aks get-credentials.

The question doesn't tell what Azure services AKS will be connecting to (if any). It only mentions the "Trusted Docker Registry", which doesn't mean ACR necesserily. What it does ask you are the commands for provisioning and CONNECTING to AKS cluster.
upvoted 4 times

syu31svc 2 years, 1 month ago

https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal?tabs=azure-cli

1) az ad sp create-for-rbac
2) az aks create
3) az role assignment create
upvoted 3 times

Govcomm 2 years, 1 month ago
az aks create
az aks sp create-for-rbac
az role assignment
upvoted 2 times

Lucario95 2 years, 4 months ago
As per this documentation: https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal
You could use:
1) az ad sp create-for-rbac
2) az aks create (specifying the service principal in this command)

Or
1) az aks create
2) az ad sp create-for-rbac
3) az role assignment

As the solution requires 3 steps, I'll go with the second option
upvoted 3 times

Question #46 *Topic 4*

Your company develops an app for iOS. All users of the app have devices that are members of a private distribution group in Microsoft Visual Studio App Center.
You plan to distribute a new release of the app.
You need to identify which certificate file you require to distribute the new release from App Center.
Which file type should you upload to App Center?

A. .cer

B. .pfx

C. .p12

D. .pvk

Suggested Answer: *C*
A successful IOS device build will produce an ipa file. In order to install the build on a device, it needs to be signed with a valid provisioning profile and certificate.
To sign the builds produced from a branch, enable code signing in the configuration pane and upload a provisioning profile (.mobileprovision) and a valid certificate (.p12), along with the password for the certificate.
Reference:
https://docs.microsoft.com/en-us/appcenter/build/xamarin/ios/

Community vote distribution

C (100%)

cucuff Highly Voted 4 years, 1 month ago
Correct answer is .p12

"To sign the builds produced from a branch, enable code signing in the configuration pane and upload a provisioning profile (.mobileprovision) and a valid certificate (.p12), along with the password for the certificate."
https://docs.microsoft.com/en-us/appcenter/build/xamarin/ios/
upvoted 27 times

Dev1079 3 years, 8 months ago
https://docs.microsoft.com/en-us/appcenter/distribution/groups
upvoted 1 times

syu31svc 2 years, 1 month ago
This clearly supports C as the answer
upvoted 1 times

hajurbau Most Recent 3 months ago
Selected Answer: C
Answer provided is correct.
https://learn.microsoft.com/en-us/appcenter/build/ios/code-signing

Visual studio app center is on the path way to being deprecated by 2025
https://learn.microsoft.com/en-au/appcenter/retirement
upvoted 2 times

yana_b 1 year, 1 month ago
Selected Answer: C
correct
upvoted 2 times

zellck 1 year, 3 months ago
Selected Answer: C
C is the answer.

https://learn.microsoft.com/en-us/appcenter/build/ios/code-signing#certificates-p12

upvoted 2 times

Govcomm 2 years, 1 month ago

.p12 for signing the package

upvoted 1 times

Eltooth 2 years, 4 months ago

Selected Answer: C

C is correct answer.

upvoted 2 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: C

correct answer and explanation

upvoted 4 times

lugospod 2 years, 7 months ago

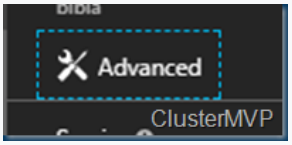
Got this January 2022.

upvoted 3 times

Question #47 *Topic 4*

SIMULATION -
You need to prepare a network security group (NSG) named az400-123456789-nsg1 to host an Azure DevOps pipeline agent. The solution must allow only the required outbound port for Azure DevOps and deny all other inbound and outbound access to the Internet.
To complete this task, sign in to the Microsoft Azure portal.

Suggested Answer: *See explanation below.*
1. Open Microsoft Azure Portal and Log into your Azure account.
2. Select network security group (NSG) named az400-123456789-nsg1
3. Select Settings, Outbound security rules, and click Add
4. Click Advanced



5. Change the following settings:
➪ Destination Port range: 8080
➪ Protocol. TCP
➪ Action: Allow
Note: By default, Azure DevOps Server uses TCP Port 8080.
Reference:
https://robertsmit.wordpress.com/2017/09/11/step-by-step-azure-network-security-groups-nsg-security-center-azure-nsg-network/
https://docs.microsoft.com/en-us/azure/devops/server/architecture/required-ports?view=azure-devops

Root_Access Highly Voted 4 years, 3 months ago
The goal is installing an agent on your cloud VM (could be on prem as well), you need to open only and only port 443 outbound.
People are mistaken because they think the goal is deploying an Azure DevOps Server.
Here is what Azure DevOps Server is:
Developers can work in the cloud using Azure DevOps Services or on-premises using Azure DevOps Server. Azure DevOps Server was formerly named Visual Studio Team Foundation Server (TFS).

https://docs.microsoft.com/en-us/azure/devops/user-guide/what-is-azure-devops?toc=%2Fazure%2Fdevops%2Fserver%2Ftoc.json&bc=%2Fazure%2Fdevops%2Fserver%2Fbreadcrumb%2Ftoc.json&view=azure-devops
upvoted 16 times

Hgreg 9 months ago
Exactly. Only 443 outbound is needed. Current documentation (as of December 2023):
https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/agents?view=azure-devops&tabs=yaml%2Cbrowser#communication-with-azure-pipelines
upvoted 2 times

zellck Highly Voted 1 year, 3 months ago
Gotten this in Jun 2023 exam.
upvoted 9 times

yana_b 1 year, 1 month ago
May you please specify the steps which you used for this lab?
Thank you!
upvoted 1 times

chakanirban Most Recent 2 months, 3 weeks ago
NO LAB on 6/21 - 9 am IST -
1 Case study , 6 new Q

1 YES NO series was new - 3 Q - I answered all No , because 2 will No and 1 Y
JOB A depends JOB B
JOB B on JOB C
JOB C on JOB D

who is dependent , who can run parallel
3 yes/ no
upvoted 2 times

son_el 4 months, 2 weeks ago
how many marks is this thing?
upvoted 1 times

yana_b 1 year, 1 month ago
The default Inbound NSG rule denies all i-net traffic, while the outbound rule allows it under Rule "AllowInternetOutBound" with priority 65001. Note that this rule refers to 'any' in regards with port, protocol and source, while sets internet for the destination => we have to create a 2nd outbound rule that denies all traffic for service tag=internet and set its priority to be lower than the rule allowing port 443.
upvoted 4 times

Sukon_Desknot 1 year, 1 month ago
Create a new network security group (NSG) named az400-123456789-nsg1 if it doesn't already exist.

Configure outbound security rules for the NSG as follows:

Name: Allow-Outbound
Priority: 100 (or any number lower than 65000)
Source: Any
Source Port Range: *
Destination: Any
Destination Port Range: 443
Protocol: TCP
Action: Allow
Configure inbound security rules to deny all inbound traffic:

Name: Deny-Inbound
Priority: 65000 (highest priority)
Source: Any
Source Port Range: *
Destination: Any
Destination Port Range: *
Protocol: *
Action: Deny
upvoted 2 times

SilentH 2 weeks, 2 days ago
Correct & complete answer. Thank you.
upvoted 1 times

xRiot007 1 year, 1 month ago
FYI - rule priority is the lower the number, the higher the priority, not the other way around. https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#:~:text=characters%20or%20%27.%27%2C%20%27%2D%27%2C%20%27_%27.-,Priority,-A%20number%20between
upvoted 1 times

chingdm 1 year, 8 months ago
should only open port 443 by default denies other ports, since it is for azure devops agent and not tfs.

"Required options
--unattended - agent setup will not prompt for information, and all settings must be provided on the command line
--url <url> - URL of the server. For example: https://dev.azure.com/myorganization or http://my-azure-devops-server:8080/tfs"

https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/v2-windows?view=azure-devops
upvoted 2 times

meoukg 1 year, 10 months ago

I saw this question in my exam lab yesterday and I created an outbound rule allow port 443
upvoted 7 times

eufdf12342 2 years, 9 months ago
Port 443!
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/agents?view=azure-devops&tabs=browser
upvoted 3 times

rdemontis 2 years, 6 months ago
thanks for sharing the document
upvoted 1 times

poplovic 2 years, 12 months ago
should be port 443 based on https://docs.microsoft.com/en-us/azure/devops/organizations/security/allow-list-ip-url?view=azure-devops&tabs=IP-V4

We recommend you open port 443 to all traffic on these IP addresses and domains. We also recommend you open port 22 to a smaller subset of targeted IP addresses.
upvoted 1 times

anchore 3 years ago
https://docs.microsoft.com/en-us/azure/devops/server/architecture/required-ports?view=azure-devops-2020
Port 8080 would be the answer
upvoted 2 times

Pamban 1 year, 3 months ago
This is the AzureDevOps server
upvoted 1 times

rg54 3 years, 1 month ago
I partly agree with Root_Access on one point : The question clearly talk about an installing an AzDO agent on a cloud VM (could be on prem as well), so needed port to connect to AzDO is 443 outbound

BUT "The solution must allow ONLY THE REQUIRED outbound port for Azure DevOps and DENY ALL OTHER inbound and outbound access to the Internet."

Moreover, default rules on NSG allow outbound traffic to Internet, and this rule cannot be deleted, only overriden :
https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#default-security-rules

-> you also have to create an outbound rule to 443, and another one with smaller priority number to deny all outbound traffic
upvoted 3 times

armvch 1 year, 10 months ago
Default rules DENY all inbound/outbound traffic, not allow. Please carefully read the description
upvoted 1 times

gulopez 3 years, 9 months ago
The Question mention "The solution must allow only the required outbound port for Azure DevOps ". So it should be port 443. If instead would say Azure DevOps Server (former TFS) then port 8080 would be the answer.
upvoted 3 times

gulopez 3 years, 9 months ago
Accordind to this documentation https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/v2-windows?view=azure-devops the the agent url uses port 8080 http://my-azure-devops-server:8080/tfs
upvoted 1 times

ttm_19 4 years, 2 months ago
The port is 443 - tested!
upvoted 4 times

yemma 4 years, 3 months ago
I think the only port needed for the azure deops agent is 443 (Tested)
But we've asked to deny everything else, one this is done we have to open for the RDP or SSH port to connect in order to install the agent.
So for me:

Inbound :
100 RDP/SSH 3389/22 Allow
110 0.0.0.0/0 * Deny
Outbound:
100 * 443 Allow
110 0.0.0.0/0 * Deny
upvoted 7 times

armvch 1 year, 10 months ago
there is a default rule for Deny All inbound traffic, no need to add additional rules for it
upvoted 6 times

rdemontis 2 years, 6 months ago
exactly, but the requirement ask only to deny all internet outboud. I think there is no need for the lab to modify inbound rules even if you are right.
upvoted 5 times

hart232 4 years, 4 months ago
Outbound:
1. Create rule to open traffic only from 8080
2. Create rule to block all outgoing traffic to internet
Inbound
1. Deny all inbound traffic from Internet

Use service tag option while creating the rule to specify the "Intternet" option.
upvoted 1 times

Question #48 *Topic 4*

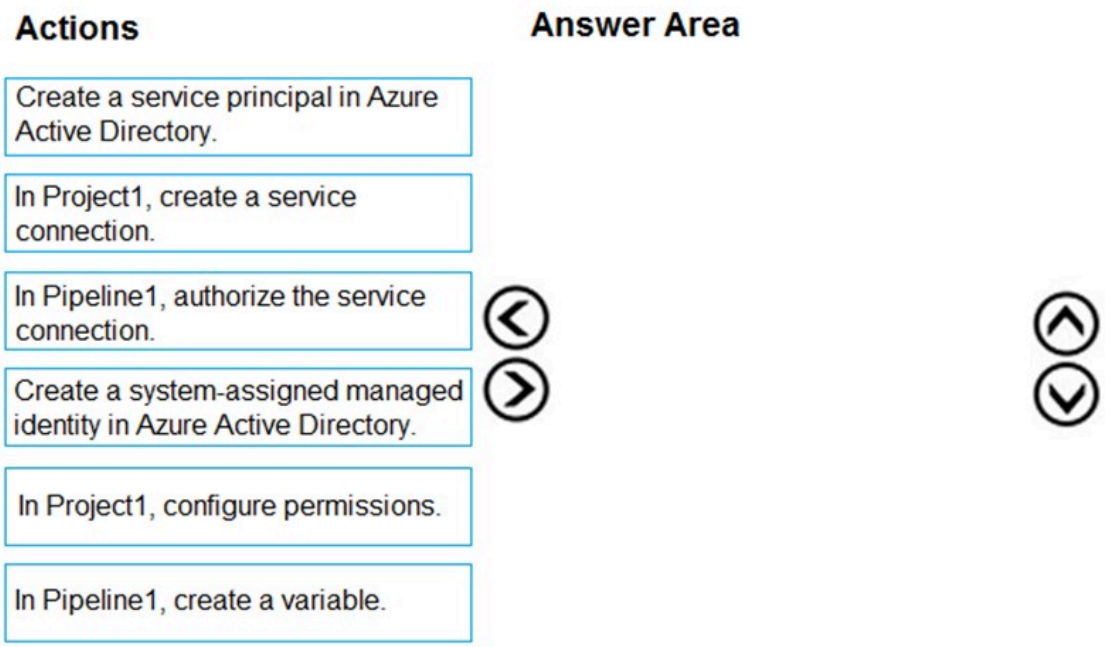
DRAG DROP -

You have a project in Azure DevOps named Project1 that contains two Azure DevOps pipelines named Pipeline1 and Pipeline2.

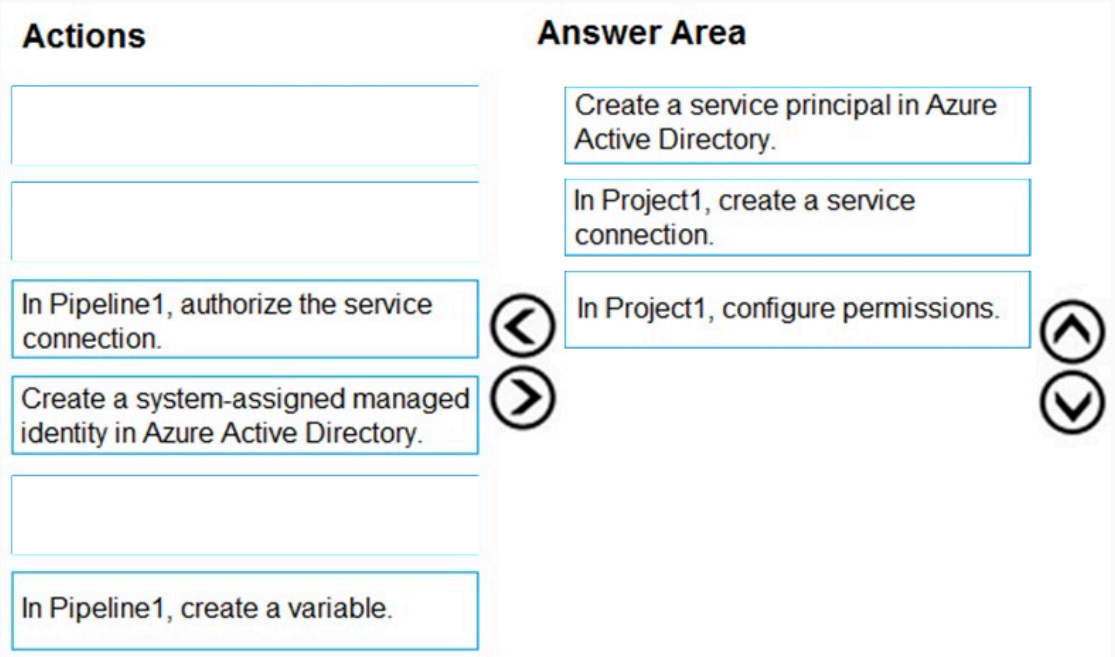
You need to ensure that Pipeline1 can deploy code successfully to an Azure web app named webapp1. The solution must ensure that Pipeline2 does not have permission to webapp1.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Suggested Answer:



Reference:

https://docs.microsoft.com/en-us/azure/devops/pipelines/library/connect-to-azure?view=azure-devops

AhmedAbouhamed Highly Voted 2 years, 10 months ago

the correct answer is below:

1- create a service principle

2- in project 1 create a service connection (ARM / Manual) and provide the service principle details created in step 1

3- in pipeline 1, authorize the service connection. this way only pipeline 1 will get access to the webapp and pipeline2 not.

also, project permissions id for users and groups not for pipelines.
I'm 100 % sure from the answer as it's repeated steps in all LABs.
upvoted 113 times

rdemontis 2 years, 6 months ago
agree with you, project permissions are for configuring Azure DevOps access from AAD Users or Groups
upvoted 1 times

UnknowMan 2 years, 4 months ago
Agree with you
upvoted 1 times

[Removed] 2 years, 9 months ago
I agree fully with you! Below comments are fake, i dont know why people upvote ..
upvoted 4 times

hebertpena88 2 years, 1 month ago
I agree with you, I do this all the time
upvoted 5 times

fanq10 Highly Voted 3 years, 2 months ago
The given answer is correct, verified in azure devops
upvoted 11 times

ZodiaC 3 years, 2 months ago
Just did it on Devops its correct
upvoted 3 times

ozbonny Most Recent 6 months, 3 weeks ago
Given answer correct
upvoted 1 times

vsvaid 9 months ago
--Create service principle, Make sure to uncheck the box "Grant access permission to all pipelines". This way we have not granted permission to any pipeline
--Click on the newly created service connection. Open security of security of pipeline. Under pipeline, add the pipeline you want .
upvoted 1 times

varinder82 9 months, 3 weeks ago
Final answer after going through all the comments

- Answer provided by examtopic is correct
upvoted 3 times

resonant 1 year, 2 months ago
Why not creating a system-assigned managed identity? Aren't managed identities superior to service principals and encouraged by Microsoft as long as you can use it? You create the managed identity for the Azure web app, don't you?
upvoted 3 times

Bear_Polar 11 months, 2 weeks ago
You cannot use managed identity with pipeline (except the case that you use VMs as build agents then you can use managed identity assigned to VMs). In this case, you have 2 options: 1. automatic authentication using signed-in credentials or 2. using custom service principle.
upvoted 4 times

icedog 1 year, 4 months ago
Suggested answer is correct.
Configure the permissions part is explained here:
https://learn.microsoft.com/en-us/azure/devops/pipelines/library/service-endpoints?view=azure-devops&tabs=classic#secure-a-service-connection
upvoted 3 times

syu31svc 2 years, 1 month ago
1) Create service principal
2) Create service connection
3) Authorize connection

https://docs.microsoft.com/en-us/azure/devops/pipelines/library/service-endpoints?view=azure-devops&tabs=classic

"To authorize a service connection for a specific pipeline, open the pipeline by selecting Edit and queue a build manually. You see a resource authorization error and an "Authorize resources" action on the error. Choose this action to explicitly add the pipeline as an authorized user of the service connection."

upvoted 4 times

Govcomm 2 years, 1 month ago

service principal
project 1 --> service connection
pipeline 1 --> authorize the service connection

upvoted 4 times

[Removed] 2 years, 9 months ago

So when creating a SP in AZ DevOps manual or automatic (Security checkbox - Grant access permission to all pipelines) is not checked!

Configuring permission in Project1 will not help here because permissions are for users and access to the project itself.

So the most logical and correct answer would be to create SP in AD, then in Project1 create a Service Connection, and then in Project1 you authorize the SP, that way only pipeline where you authorised SP will be able to use it and not other.

upvoted 5 times

Aelx 3 years, 2 months ago

1. Create Service connection
2. Project level permissions
3. Authorize the service connection

https://docs.microsoft.com/en-us/azure/devops/pipelines/library/service-endpoints?view=azure-devops&tabs=classic

upvoted 5 times

Sandy_29 3 years, 2 months ago

I guess

D
B
C

any suggestion?

upvoted 2 times

SSTan 3 years, 2 months ago

what could be the answer?

upvoted 1 times

Question #49 *Topic 4*

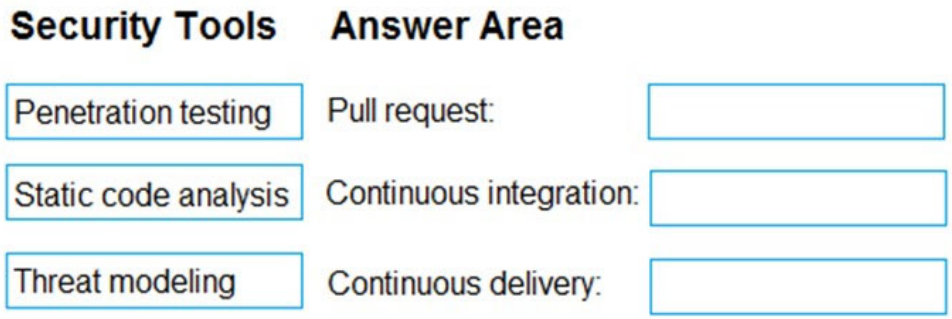
DRAG DROP -

You need to increase the security of your team's development process.

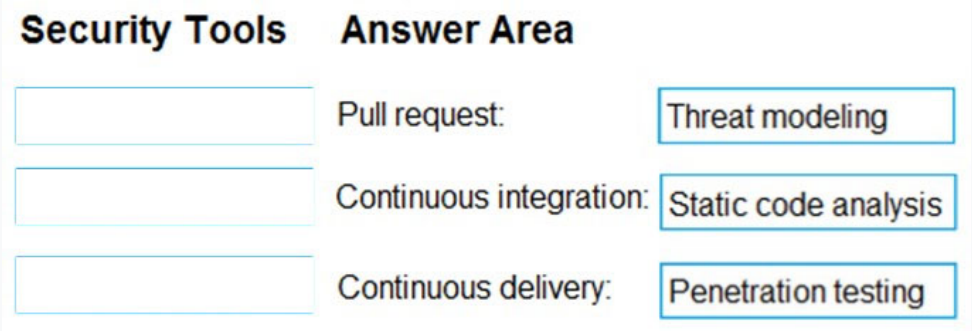
Which type of security tool should you recommend for each stage of the development process? To answer, drag the appropriate security tools to the correct stages. Each security tool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested Answer:



Box 1: Threat modeling -

Threat modeling's motto should be, ı€The earlier the better, but not too late and never ignore.ı€

Box 2: Static code analysis -

Validation in the CI/CD begins before the developer commits his or her code. Static code analysis tools in the IDE provide the first line of defense to help ensure that security vulnerabilities are not introduced into the CI/CD process.

Box 3: Penetration testing -

Once your code quality is verified, and the application is deployed to a lower environment like development or QA, the process should verify that there are not any security vulnerabilities in the running application. This can be accomplished by executing automated penetration test against the running application to scan it for vulnerabilities.

Reference:

https://docs.microsoft.com/en-us/azure/devops/articles/security-validation-cicd-pipeline?view=vsts

rengs Highly Voted 3 years, 2 months ago

Static code

Static code

Penetration

https://docs.microsoft.com/en-us/azure/devops/migrate/security-validation-cicd-pipeline?view=azure-devops#ide--pull-request

upvoted 68 times

rdemontis 2 years, 6 months ago

totally agree with you

upvoted 1 times

ZodiaC 3 years, 2 months ago

1000% CORRECT

upvoted 5 times

PlumpyTumbler Highly Voted 2 years, 7 months ago

The officially sanctioned practice test for this exam on measureup.com has this question. The answers are
Pull Request: Static code analysis
CI: package vulnerability
CD: Pentest

That means that Microsoft recognizes those as the correct answers. If the newest version of the test says package vulnerability instead of threat modeling, choose it.
upvoted 26 times

xRiot007 1 year, 2 months ago
Threat modeling is one thing, vulnarability scanning is a totally other thing. Vulnerability scanning is part of static scans, so first 2 points are SCA, SCA, then you do penetration testing during Continuous Delivery, after the build is over.
upvoted 1 times

ozbonny Most Recent 6 months, 3 weeks ago
maybe this could be the explanation of examtopics

Threat modeling is typically conducted during the design and planning phases of software development to identify potential security threats and vulnerabilities in a system. While it's not common to perform threat modeling directly within a pull request (PR) itself, the findings from threat modeling activities can certainly inform the development process, including code reviews and pull requests.
upvoted 1 times

ozbonny 6 months, 3 weeks ago
According with this documentation I think is
static code
static code
penetration

https://learn.microsoft.com/en-us/training/modules/static-analyzers/4-manage-technical-debt-sonarcloud-azure-devops
https://www.imperva.com/learn/application-security/penetration-testing/
upvoted 1 times

ozbonny 6 months, 3 weeks ago
According with this documentation I think is
static code
static code
penetration

https://learn.microsoft.com/en-us/training/modules/static-analyzers/4-manage-technical-debt-sonarcloud-azure-devops
upvoted 1 times

CirusD 11 months, 3 weeks ago
Pull Request: Static code analysis
Continuous Integration: Threat modelling
Continuous Delivery: Penetration testing
upvoted 1 times

yana_b 1 year, 1 month ago
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls#static-application-security-testing
https://learn.microsoft.com/en-us/azure/devops/pipelines/security/overview?view=azure-devops#ide--pull-request
Seems that Box1 should be static code. The other 2 answer options seem to be correct.
upvoted 1 times

ieboaix 1 year, 1 month ago
Threat modeling is recommended to be done in design & planning stage. according to OWASP some refined measures can also be done in other stages. CI CD should only have automated tools, PR is possible, but if ask a recommendation, it should be done before PR. so it should be
Static code
Static code
Penetration
upvoted 2 times

zellck 1 year, 3 months ago

1. Static code analysis
2. Static code analysis
3. Penetration testing

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls#static-application-security-testing
But a team must start somewhere when implementing static code scanning practices. One way is to introduce static code analysis inside of continuous integration. This method verifies security as soon as code changes happen. One example is SonarCloud. It wraps multiple static application security testing (SAST) tools for different languages. SonarCloud assesses and tracks technical debt with a focus on maintainability. It looks at code quality and style and has security-specific checkers. But there are many other commercial and open-source tools available in the market.
upvoted 5 times

dmeld 1 year, 10 months ago
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls
The given answer is correct.
Pull requests are standard in the development process. Part of the pull request process is peer reviews that often reveal undiscovered defects, bugs, or issues related to human mistakes. It's good practice to have a security champion or knowledgeable security teammate who can guide the developer during the peer review process before creating a pull request.

Secure coding practice guidelines help developers learn essential secure coding principles and how they should be applied. There are secure coding practices available, such as OWASP secure coding practices to incorporate with general coding practices.
upvoted 3 times

Mattt 4 months ago
I also blieve that the given answer is correct.
upvoted 1 times

syu31svc 2 years, 1 month ago
Did a course on Cloud Guru

Answer is as follows

Pull request ---> static code analysis
Continuous Integration ---> static code analysis
Continuous delivery ---> Penetration testing
upvoted 6 times

Govcomm 2 years, 1 month ago
Thread modelling
Static code analysis
Penetration testing
upvoted 2 times

Inland 2 years, 2 months ago
Given answers are correct.
https://www.synopsys.com/blogs/software-security/threat-modeling-sdlc/#:~:text=While%20threat%20modeling%20should%20take,modeling%20within%20the%20support%20cycle.
https://docs.microsoft.com/en-us/azure/security/develop/security-code-analysis-overview
upvoted 1 times

Eltooth 2 years, 4 months ago
Static
Static
Pen test
upvoted 3 times

Cheehp 2 years, 5 months ago
Selected during exam.
Static code analysis
Static code analysis
Penetration testing
upvoted 5 times

d0bermannn 2 years, 11 months ago

Static code

Threat modeling

Penetration

upvoted 2 times

sanhoo 3 years, 1 month ago

Threat modeling: - It is usually a manual process and done as part of PR review

Static code- During the build phase using tools like sonarqube

Penetration:- once code is build and ready for deployment we check if the that it is free from web attacks

upvoted 13 times

xRiot007 1 year, 2 months ago

Wrong. This is what threat modelling is : https://www.synopsys.com/glossary/what-is-threat-modeling.html#E

upvoted 1 times

Question #50 *Topic 4*

Your company is concerned that when developers introduce open source libraries, it creates licensing compliance issues.
You need to add an automated process to the build pipeline to detect when common open source libraries are added to the code base.
What should you use?

A. OWASP ZAP

B. Jenkins

C. Code Style

D. WhiteSource Bolt

Suggested Answer: *D*
WhiteSource provides WhiteSource Bolt, a lightweight open source security and management solution developed specifically for integration with Azure DevOps and Azure DevOps Server.
Note: WhiteSource is the leader in continuous open source software security and compliance management. WhiteSource integrates into your build process, irrespective of your programming languages, build tools, or development environments. It works automatically, continuously, and silently in the background, checking the security, licensing, and quality of your open source components against WhiteSource constantly-updated definitive database of open source repositories.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. Black Duck
2. WhiteSource Bolt
Other incorrect answer options you may see on the exam include the following:
1. Microsoft Visual SourceSafe
2. PDM
3. SourceGear
4. SourceGear Vault
Reference:
https://www.azuredevopslabs.com/labs/vstsextend/whitesource/

Community vote distribution

D (100%)

francis6170 Highly Voted 3 years, 2 months ago
Got this in the AZ-400 exam (June 2021), but option was Black Duck instead of WhiteSource Bolt.
upvoted 14 times

Kazillius 3 years, 2 months ago
There is another question in this dump that has Black Duck as answer instead of WhiteSource Bolt.
upvoted 10 times

ukohae39 Highly Voted 3 years, 2 months ago
WhiteSource Bolt or Black Duck is Correct and Verified!
upvoted 9 times

zellck Most Recent 1 year, 3 months ago
Selected Answer: D
D is the answer.

https://marketplace.visualstudio.com/items?itemName=whitesource.whitesource
WhiteSource integrates with your CI servers, build tools and repositories to detect all open source components in your software, without ever scanning your code. It provides you with real-time alerts on vulnerable or problematic components, generates comprehensive up-to-date reports in one-click and enables you to streamline your entire open source management process with automated policies.
upvoted 3 times

syu31svc 2 years, 1 month ago
Selected Answer: D
100% D

upvoted 1 times

Govcomm 2 years, 1 month ago

Build pipeline WhiteSource Bolt

upvoted 1 times

Eltooth 2 years, 4 months ago

Selected Answer: D

D is correct answer.

upvoted 1 times

UnknowMan 2 years, 4 months ago

Selected Answer: D

Correct

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: D

provided answer is correct

upvoted 1 times

eufdf12342 2 years, 9 months ago

Selected Answer: D

Correct

upvoted 2 times

Kalaismile06 3 years, 1 month ago

Got this question in AZ-400(July exam)

upvoted 2 times

davidy2020 3 years, 3 months ago

https://docs.microsoft.com/en-us/visualstudio/subscriptions/vs-whitesource

upvoted 1 times

Miles19 3 years, 5 months ago

Correct

upvoted 4 times

s_trichkov 3 years, 5 months ago

Correctamundo dude

upvoted 1 times

umer123 3 years, 5 months ago

correct

upvoted 3 times

Question #51 *Topic 4*

You plan to use a NuGet package in a project in Azure DevOps. The NuGet package is in a feed that requires authentication.
You need to ensure that the project can restore the NuGet package automatically.
What should the project use to automate the authentication?

A. an Azure Automation account

B. an Azure Artifacts Credential Provider

C. an Azure Active Directory (Azure AD) account that has multi-factor authentication (MFA) enabled

D. an Azure Active Directory (Azure AD) service principal

Suggested Answer: *B*
The Azure Artifacts Credential Provider automates the acquisition of credentials needed to restore NuGet packages as part of your .NET development workflow. It integrates with MSBuild, dotnet, and NuGet(.exe) and works on Windows, Mac, and Linux. Any time you want to use packages from an Azure Artifacts feed, the
Credential Provider will automatically acquire and securely store a token on behalf of the NuGet client you're using.
Reference:
https://github.com/Microsoft/artifacts-credprovider

Community vote distribution

B (100%)

Bronskins Highly Voted 3 years, 11 months ago
Correct!
upvoted 20 times

zellck Highly Voted 1 year, 3 months ago
Selected Answer: B
B is the answer.

https://github.com/microsoft/artifacts-credprovider#azure-artifacts-credential-provider
The Azure Artifacts Credential Provider automates the acquisition of credentials needed to restore NuGet packages as part of your .NET development workflow. It integrates with MSBuild, dotnet, and NuGet(.exe) and works on Windows, Mac, and Linux. Any time you want to use packages from an Azure Artifacts feed, the Credential Provider will automatically acquire and securely store a token on behalf of the NuGet client you're using.
upvoted 5 times

zellck 1 year, 3 months ago
Gotten this in Jun 2023 exam.
upvoted 4 times

renzoku Most Recent 1 year, 2 months ago
Selected Answer: B
B. an Azure Artifacts Credential Provider
Retrieve and manage the necessary credentials to access the package feed.
Integrates with various package managers like NuGet, npm, and Maven.
Ensure that the project can automatically restore the NuGet package without requiring manual authentication each time.

Azure AD service principal, typically used for programmatic authentication and authorization in Azure services.
upvoted 2 times

syu31svc 2 years, 1 month ago
Selected Answer: B
B is correct as supported by given explanation
upvoted 2 times

Govcomm 2 years, 1 month ago
Azure artifact credential provider
upvoted 2 times

lindo1213 2 years, 2 months ago

Correct answer

upvoted 1 times

Eltooth 2 years, 4 months ago

Selected Answer: B

B is correct answer.

upvoted 2 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: B

correct

upvoted 2 times

Honeywell_EMP 2 years, 6 months ago

Selected Answer: B

Correct.

upvoted 1 times

shermin1 2 years, 6 months ago

Came in exam march 13....

upvoted 4 times

Whirly 2 years, 5 months ago

Thanks for posting the exam appeared questions, very helpful.

upvoted 3 times

eddy_040695 3 years ago

Correct

upvoted 1 times

goatlord 3 years, 1 month ago

Ultra Correct

upvoted 2 times

AshrafAli 3 years, 3 months ago

Correct

upvoted 2 times

Question #52 *Topic 4*

You use Azure Pipelines to manage project builds and deployments.
You plan to use Azure Pipelines for Microsoft Teams to notify the legal team when a new build is ready for release.
You need to configure the Organization Settings in Azure DevOps to support Azure Pipelines for Microsoft Teams.
What should you turn on?

A. Third-party application access via OAuth

B. Azure Active Directory Conditional Access Policy Validation

C. Alternate authentication credentials

D. SSH authentication

Suggested Answer: *A*
The Azure Pipelines app uses the OAuth authentication protocol, and requires Third-party application access via OAuth for the organization to be enabled. To enable this setting, navigate to Organization Settings > Security > Policies, and set the Third-party application access via OAuth for the organization setting to On.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/integrations/microsoft-teams

Community vote distribution
A (100%)

Hooters Highly Voted 3 years, 10 months ago
A. Third party application access via OAuth' must be enabled to receive notifications for the organization in Azure DevOps (Organization Settings -> Security -> Policies)
https://docs.microsoft.com/en-us/azure/devops/pipelines/integrations/microsoft-teams?view=azure-devops
upvoted 18 times

francis6170 Highly Voted 3 years, 2 months ago
Got this in the AZ-400 exam (June 2021).
upvoted 12 times

Skankhunt Most Recent 1 month, 3 weeks ago
Old question, answer now would be something like "Create new Teams Service hook in Project settings"
upvoted 1 times

zellck 1 year, 3 months ago
Selected Answer: A
A is the answer.

https://learn.microsoft.com/en-us/azure/devops/service-hooks/authorize?view=azure-devops
When you use a service that's integrated with Azure DevOps, the industry-standard OAuth 2.0 authorization framework provides safe and secure access to your resources by those other services. With OAuth, you grant a service the authorization to access your Azure DevOps resources, such as work items, source code, and build results.
upvoted 3 times

syu31svc 2 years, 1 month ago
Selected Answer: A
https://docs.microsoft.com/en-us/azure/devops/pipelines/integrations/media/troubleshooting/third-party-app-consent.png?view=azure-devops

A is the answer
upvoted 3 times

Govcomm 2 years, 1 month ago
Third-party application access via OAuth
upvoted 1 times

Eltooth 2 years, 4 months ago
Selected Answer: A

A is correct answer.
upvoted 3 times

AnshMan 2 years, 4 months ago

Selected Answer: A

Azure DevOps no longer supports Alternate Credentials authentication since the beginning of March 2, 2020.
Third-party application via OAuth - Enable third-party applications to access resources in your organization through OAuth.
SSH Authentication - Enable applications to connect to your organization's Git repos through SSH.

So Answer is "A" Third-party application access via OAuth

https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/change-application-access-policies?view=azure-devops
upvoted 3 times

rdemontis 2 years, 6 months ago

Selected Answer: A

correct answer
https://docs.microsoft.com/en-us/azure/devops/pipelines/integrations/microsoft-teams?view=azure-devops#use-commands
upvoted 1 times

subrata83 2 years, 11 months ago

Got this in the Az-400 exam(Sep 27 2021)
upvoted 3 times

Kalaismile06 3 years, 2 months ago

Got this in the Az-400 exam(July 2021)
upvoted 5 times

27close 3 years, 10 months ago

Answer A- see the link
upvoted 2 times

27close 3 years, 10 months ago

You can use the Azure Pipelines app for Microsoft Teams only with a project hosted on Azure DevOps Services at this time.'Third party application access via OAuth' must be enabled to receive notifications for the organization in Azure DevOps (Organization Settings -> Security -> Policies).
https://docs.microsoft.com/en-us/azure/devops/pipelines/integrations/microsoft-teams?view=azure-devops
upvoted 3 times

Question #53 *Topic 4*

You have an existing project in Azure DevOps.
You plan to integrate GitHub as the repository for the project.
You need to ensure that Azure Pipelines runs under the Azure Pipelines identity.
Which authentication mechanism should you use?

A. personal access token (PAT)

B. GitHub App

C. Azure Active Directory (Azure AD)

D. OAuth

Suggested Answer: *B*
GitHub App uses the Azure Pipelines identity.
Incorrect Answers:
A: Personal access token and OAuth use your personal GitHub identity.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/repos/github

Community vote distribution
B (100%)

eray95 Highly Voted 3 years, 10 months ago
B correct answer. Initially I' m confused little but to ensure that Pipelines run using The Azure Pipelines identity clearly show the given answer is right https://docs.microsoft.com/en-us/azure/devops/pipelines/repos/github?view=azure-devops&tabs=yaml
upvoted 15 times

Hooters 3 years, 10 months ago
Seems correct as per the reference article.
upvoted 1 times

27close Highly Voted 3 years, 10 months ago
Authentication type Pipelines run using Works with GitHub Checks
1. GitHub App The Azure Pipelines identity Yes
2. OAuth Your personal GitHub identity No
3. Personal access token (PAT) Your personal GitHub identity
upvoted 12 times

husam421 Most Recent 2 months, 2 weeks ago
Selected Answer: B
Authentication type Pipelines run using Works with GitHub Checks
1. GitHub App The Azure Pipelines identity Yes
2. OAuth Your personal GitHub identity No
3. Personal access token (PAT) Your personal GitHub identity No
upvoted 1 times

sandyaqua 5 months, 3 weeks ago
Selected Answer: B
B. GitHub App

The Azure Pipelines GitHub App is the recommended authentication type for continuous integration pipelines. After you install the GitHub App in your GitHub account or organization, your pipeline will run without using your personal GitHub identity. Builds and GitHub status updates will be performed using the Azure Pipelines identity. This allows for a clear separation between personal and automated actions, providing better security and management of access rights within your project's CI/CD processes.
upvoted 3 times

resonant 1 year ago
I had a similar question to this one on my exam on September 12, 2023, but it asked something along the lines of which authentication method to use if the pipelines needs access to external services. The Github App option wasn't there (Now that I think about it, I think the question didn't

mention Github at all, but I'm not sure) and I choosed the PAT token. Passed with 877.
upvoted 5 times

renzoku 1 year, 2 months ago

Selected Answer: B

B. GitHub App:
Allows Azure Pipelines run with its own identity and access permissions when interacting with the GitHub repository.

Personal Access Token (PAT), Azure Pipelines will have access to GitHub using the the permissions associated with the PAT.
Azure AD, it isn't the preferred authentication mechanism for integrating GitHub repositories with Azure Pipelines.
OAuth, Used to authenticate users and services with GitHub, Not ensure using the Azure Pipelines identity.
upvoted 2 times

zellck 1 year, 3 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/devops/pipelines/repos/github?view=azure-devops&tabs=yaml#github-app-authentication
The Azure Pipelines GitHub App is the recommended authentication type for continuous integration pipelines.
upvoted 2 times

MSlave 1 year, 5 months ago

Selected Answer: B

The Azure Pipelines GitHub App is the recommended authentication type for continuous integration pipelines. After you install the GitHub App in your GitHub account or organization, your pipeline will run without using your personal GitHub identity. Builds and GitHub status updates will be performed using the Azure Pipelines identity. The app works with GitHub Checks to display build, test, and code coverage results in GitHub.

https://learn.microsoft.com/en-us/azure/devops/pipelines/repos/github?view=azure-devops&tabs=yaml#github-app-authentication
upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: B

https://docs.microsoft.com/en-us/azure/devops/pipelines/repos/github?view=azure-devops&tabs=yaml

"The Azure Pipelines GitHub App is the recommended authentication type for continuous integration pipelines."

Answer is B
upvoted 1 times

tjeerd 2 years, 1 month ago

Selected Answer: B

On exam 20220727.
upvoted 1 times

Govcomm 2 years, 1 month ago

GitHub App
upvoted 1 times

Eltooth 2 years, 4 months ago

Selected Answer: B

B is correct answer.
upvoted 2 times

rdemontis 2 years, 6 months ago

Selected Answer: B

correct answer
https://docs.microsoft.com/en-us/azure/devops/pipelines/repos/github?view=azure-devops&tabs=yaml
upvoted 1 times

Optimist_Indian 2 years, 7 months ago

Got this question in Feb-2022 exam (scored 910+). Given answer is correct. Github APP.
upvoted 4 times

rsamant 2 years, 11 months ago

A is corect

Authentication type Pipelines run using Works with GitHub Checks
1. GitHub App The Azure Pipelines identity Yes
2. OAuth Your personal GitHub identity No
3. Personal access token (PAT) Your personal GitHub identity No

https://docs.microsoft.com/en-us/azure/devops/pipelines/repos/github?view=azure-devops&tabs=yaml
upvoted 2 times

rsamant 2 years, 11 months ago
sorry i meant B. Github App
upvoted 1 times

Art3 2 years, 7 months ago
B is correct.
upvoted 1 times

subrata83 2 years, 11 months ago
Got this in the Az-400 exam(Sep 27 2021)
upvoted 6 times

azureSkies13 3 years ago
The links have the info but its a long article. Look for the "Access to GitHub repositories" it has a table with details
upvoted 2 times

DRAG DROP -

You have an Azure subscription that uses Azure Monitor and contains a Log Analytics workspace.

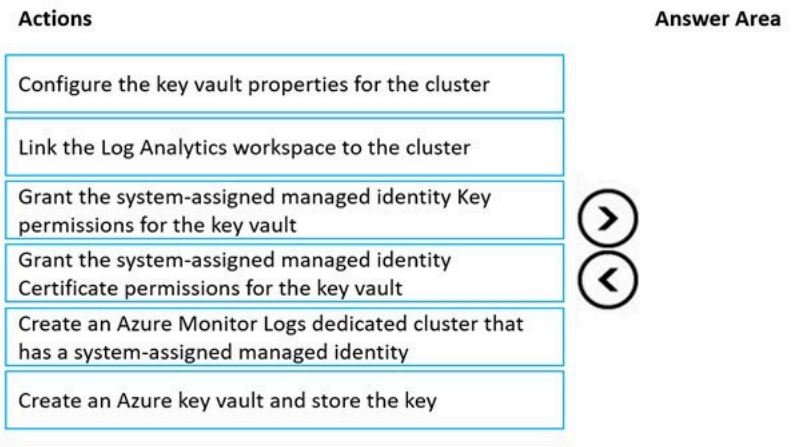
You have an encryption key.

You need to configure Azure Monitor to use the key to encrypt log data.

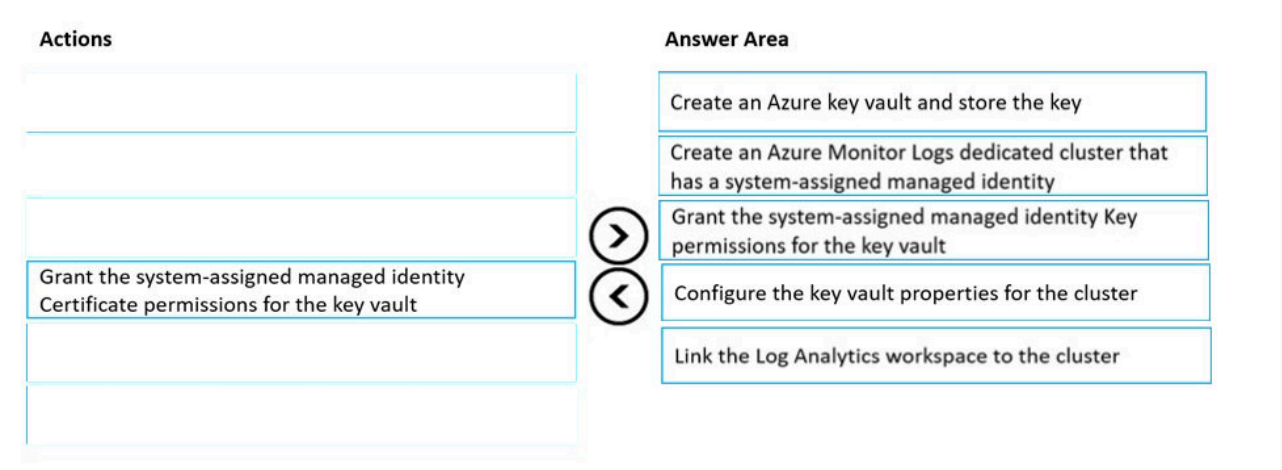
Which five actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Select and Place:



Suggested Answer:



Customer-Managed key provisioning steps:

Step 1: Create an Azure Key vault and store the key.

Creating Azure Key Vault and storing key. Create or use an existing Azure Key Vault in the region that the cluster is planed, and generate or import a key to be used for logs encryption.

Step 2: Create an Azure Monitor Logs dedicate cluster that has a system-assigned managed identity

Clusters uses managed identity for data encryption with your Key Vault. Configure identity type property to SystemAssigned when creating your cluster to allow access to your Key Vault for "wrap" and "unwrap" operations.

Step 3: Grant the system-assigned managed Identity Key permissions for the key vault.

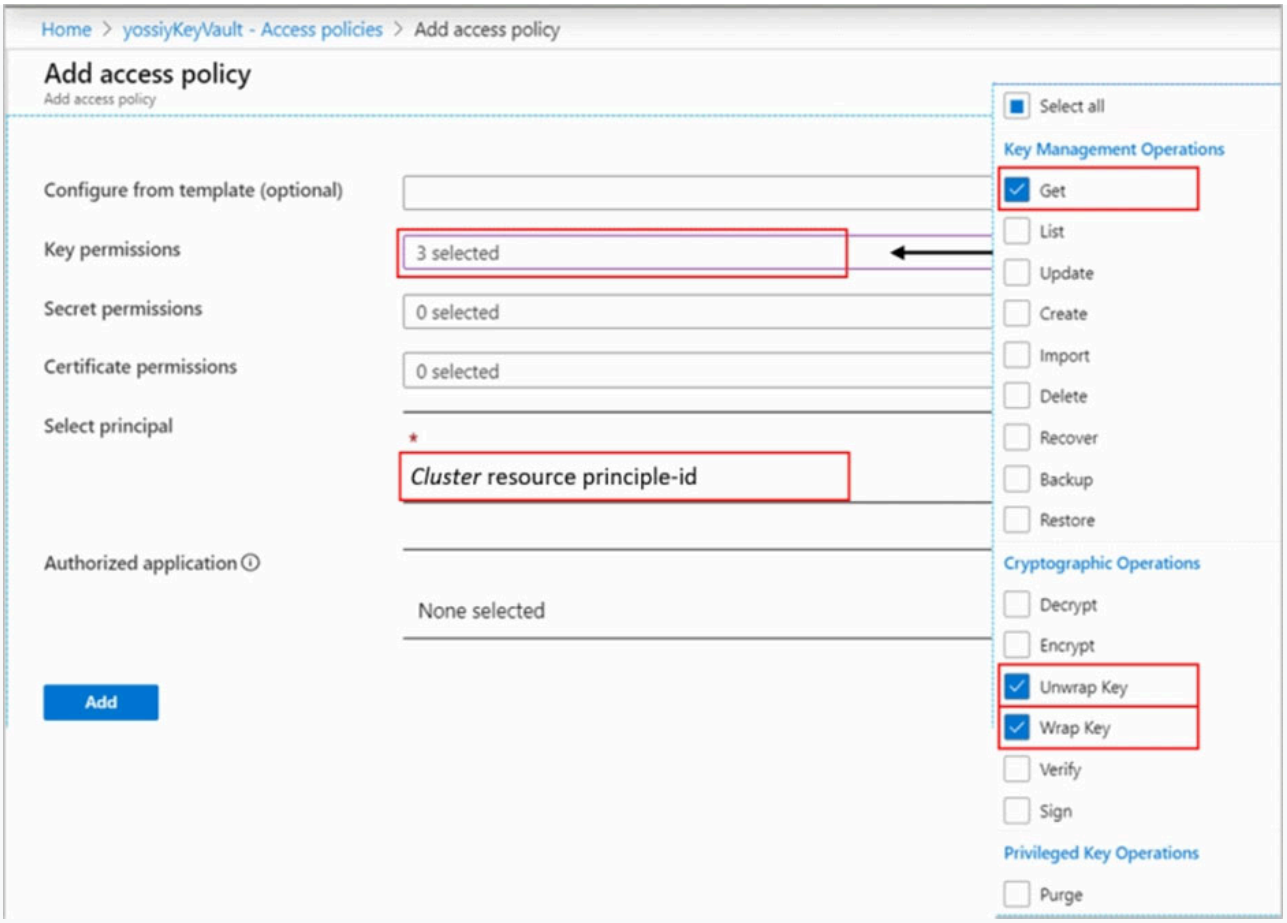
Grant Key Vault permissions.

Create Access Policy in Key Vault to grants permissions to your cluster. These permissions are used by the underlay cluster storage. Open your Key Vault in

Azure portal and click Access Policies then + Add Access Policy to create a policy with these settings:

Key permissionsƷ€"select Get, Wrap Key and Unwrap Key.

Etc.



1. Creating cluster
2. Granting permissions to your Key Vault
3. Updating cluster with key identifier details
4. Linking workspaces

Step 4: Configure the key vault properties for the cluster.

Update cluster with key identifier details.

Step 5: Link the Log Analytics workspace to the cluster

Link workspace to cluster.

This step should be performed only after the cluster provisioning. If you link workspaces and ingest data prior to the provisioning, ingested data will be dropped and won't be recoverable.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/logs/customer-managed-keys

resonant Highly Voted 1 year ago

This question was on my exam on September 12, 2023. Choosed the given answer and passed with 877.

upvoted 13 times

syu31svc Highly Voted 2 years ago

Given answer is correct and is supported by given link plus explanation

upvoted 8 times

Dimedrol1 Most Recent 8 months, 1 week ago

Considering the statement "More than one order of answer choices is correct," the steps "Creating an Azure Monitor Logs dedicated cluster" and "Create an Azure key vault and store the key" can be performed in any sequence.

As per the documentation (https://learn.microsoft.com/en-us/azure/azure-monitor/logs/logs-dedicated-clusters?tabs=cli),
Creating an Azure Monitor Logs dedicated cluster doesn't require a predefined key.
This means we can first set up the cluster and then create the Key Vault.

My answer:

- Create an Azure Monitor Logs dedicated cluster
- Create an Azure key vault and store the key

- Grant the system-assigned managed identity Key permissions
- Configure the key vault properties for the cluster
- Link the Log Analytics workspace to the cluster

upvoted 1 times

vsvaid 9 months ago

ExamTopics seems correct as per article this https://learn.microsoft.com/en-us/azure/azure-monitor/logs/customer-managed-keys?tabs=portal

---

Customer-Managed key provisioning steps
Creating Azure Key Vault and storing key
Creating cluster
Granting permissions to your Key Vault
Updating cluster with key identifier details
Linking workspaces

upvoted 1 times

varinder82 9 months, 3 weeks ago

Final answer after all the comments
- Answer provided by examtopic is correct

upvoted 3 times

flafernan 1 year, 1 month ago

Issues surrounding the specific sequence of steps to configure services on Azure can be tricky as they can vary depending on specific environment requirements and security policies. These questions can lead to ambiguous or subjective answers, which can make the assessment more difficult for candidates.

upvoted 3 times

yana_b 1 year, 1 month ago

@zellck, did you have simulations and if yes, how many and were they from the exam topics site?
Thank you!

upvoted 1 times

zellck 1 year, 3 months ago

1. Create Azure key vault and store key
2. Create Azure Monitor Logs dedicated cluster with system-assigned managed identity
3. Grant system-assigned managed identity key permissions for key vault
4. Configure key vault properties for cluster
5. Link the Log Analytics workspace to cluster

https://learn.microsoft.com/en-us/azure/azure-monitor/logs/customer-managed-keys?tabs=portal#customer-managed-key-provisioning-steps
- Creating Azure Key Vault and storing key
- Creating cluster
- Granting permissions to your Key Vault
- Updating cluster with key identifier details
- Linking workspaces

upvoted 7 times

zellck 1 year, 3 months ago

Gotten this in Jun 2023 exam.

upvoted 6 times

itbrpl 1 year, 6 months ago

I am missing te cluster information on the question.. which cluster? Questions is about Azure Monitore and Log Workspace

upvoted 5 times

Darkeh 1 year, 12 months ago

Customer-Managed key provisioning steps:
Creating Azure Key Vault and storing key
Creating cluster
Granting permissions to your Key Vault
Updating cluster with key identifier details
Linking workspaces

upvoted 6 times

DRAG DROP -

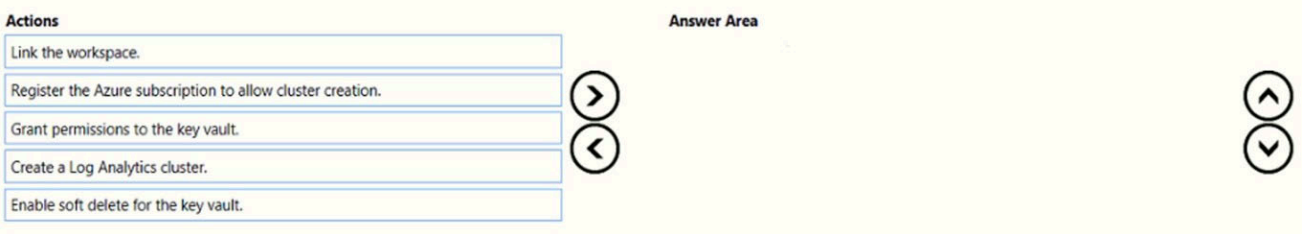
You have an Azure Key Vault that contains an encryption key named key1.

You plan to create a Log Analytics workspace that will store logging data.

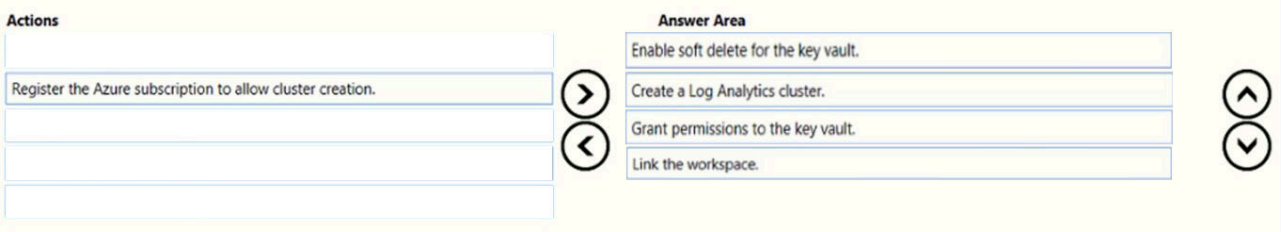
You need to encrypt the workspace by using key1.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Suggested Answer:



Customer-Managed key provisioning steps (assuming there already is an Azure Key Vault):

Step 1: Enable soft delete for the key vault.

The Azure Key Vault must be configured as recoverable, to protect your key and the access to your data in Azure Monitor. You can verify this configuration under properties in your Key Vault, both Soft delete and Purge protection should be enabled.

Step 2: Create a Log Analytics cluster.

Clusters uses managed identity for data encryption with your Key Vault. Configure identity type property to SystemAssigned when creating your cluster to allow access to your Key Vault for "wrap" and "unwrap" operations.

Step 3: Grant permissions to the key vault.

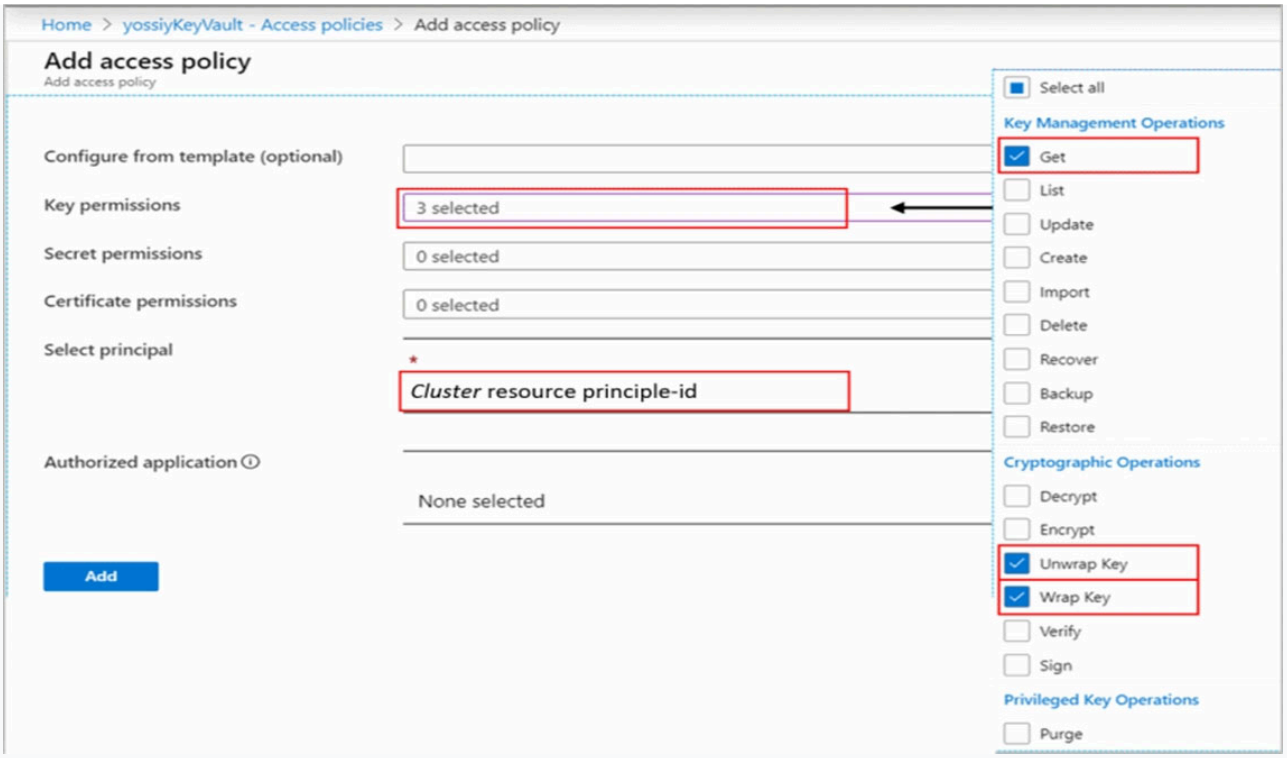
Grant Key Vault permissions.

Create Access Policy in Key Vault to grants permissions to your cluster. These permissions are used by the underlay cluster storage. Open your Key Vault in

Azure portal and click Access Policies then + Add Access Policy to create a policy with these settings:

Key permissionsา€"select Get, Wrap Key and Unwrap Key.

Etc.



1. Creating cluster
2. Granting permissions to your Key Vault
3. Updating cluster with key identifier details
4. Linking workspaces

Step 4: Link workspace -
Link workspace to cluster.
This step should be performed only after the cluster provisioning. If you link workspaces and ingest data prior to the provisioning, ingested data will be dropped and won't be recoverable.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/logs/customer-managed-keys

509325_5153 Highly Voted 1 year, 11 months ago
Why do we need soft delete?

I was thinking...
1. Register the Azure subscription to allow cluster creation.
2. Create a Log Analytics cluster.
3. Grant permissions to the key vault.
4. Link the workspace.
upvoted 52 times

RealRaymond 1 year, 4 months ago
Not able to find any reference to "Register the Azure subscription to allow cluster creation."
upvoted 2 times

Pamban 1 year, 3 months ago
here is the referance:

https://learn.microsoft.com/en-us/azure/azure-monitor/logs/logs-dedicated-clusters?tabs=cli

Cluster creation triggers resource allocation and provisioning. This operation can take a few hours to complete. Dedicated cluster is billed once provisioned regardless data ingestion and it's recommended to prepare the deployment to expedite the provisioning and workspaces link to cluster. Verify the following:

A list of initial workspace to be linked to cluster is identified
You have permissions to subscription intended for the cluster and any workspace to be linked
upvoted 2 times

armvch 1 year, 10 months ago
We already have Keyvault, why do we need to create an Azure Subs then? Enabling soft delete sounds more logical, I guess
upvoted 4 times

binhdortmund 1 year, 8 months ago
Yes, we already have Keyvault and while creating Keyvault, the Soft Delete is enable, we cant change here. So this step "Enabling soft delete" is impossible
upvoted 1 times

armvch 1 year, 6 months ago
This Keyvault could have been created before the deprecating of soft deletion optional enabling. There is a guide how to enable soft deletion for existing Keyvaults. https://learn.microsoft.com/en-us/azure/key-vault/general/soft-delete-change
Anyway, we already have some subscription because we already have Keyvault.
upvoted 2 times

binhdortmund 1 year, 8 months ago
From azure portal:
"The ability to turn off soft delete via the Azure Portal has been deprecated. You can create a new key vault with soft delete off for a limited time using CLI / PowerShell / REST API. The ability to create a key vault with soft delete disabled will be fully deprecated by the end of the year."
upvoted 5 times

Pamban 1 year, 3 months ago
Yes correct. according to below link

https://learn.microsoft.com/en-us/azure/azure-monitor/logs/logs-dedicated-clusters?tabs=cli
explanation is follows

Cluster creation triggers resource allocation and provisioning. This operation can take a few hours to complete. Dedicated cluster is billed once provisioned regardless data ingestion and it's recommended to prepare the deployment to expedite the provisioning and workspaces link to cluster. Verify the following:

A list of initial workspace to be linked to cluster is identified
You have permissions to subscription intended for the cluster and any workspace to be linked

nothing to do with soft delete here
upvoted 3 times

6c01613 6 months, 3 weeks ago
Correct
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/customer-managed-keys?tabs=portal
upvoted 1 times

Pamban Highly Voted 1 year, 2 months ago
this question appeared on today's (20/06/23) exam.selected below order. scored 955. should be correct! cheers

1. Register the Azure subscription to allow cluster creation.
2. Create a Log Analytics cluster.
3. Grant permissions to the key vault.
4. Link the workspace.

upvoted 27 times

Inderpreet773 1 year, 2 months ago
@Pamban - Could you share other questions also and any lab related quiz? And how many from examtopics?
upvoted 1 times

husam421 Most Recent 2 months ago
Given answer is correct

https://learn.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview
upvoted 1 times

hajurbau 2 months, 1 week ago

Soft Delete must be enabled as per microsoft link https://learn.microsoft.com/en-us/azure/azure-monitor/logs/logs-dedicated-clusters?tabs=azure-portal

The Azure Key Vault must be configured as recoverable, to protect your key and the access to your data in Azure Monitor. You can verify this configuration under properties in your Key Vault, both Soft delete and Purge protection should be enabled.
upvoted 1 times

hajurbau 3 months ago
Based on the Microsoft link https://learn.microsoft.com/en-us/azure/azure-monitor/logs/customer-managed-keys?tabs=portal (Check the Storage encryption key section)

The Azure Key Vault must be configured as recoverable, to protect your key and the access to your data in Azure Monitor. You can verify this configuration under properties in your Key Vault, both Soft delete and Purge protection should be enabled.
upvoted 1 times

zellck 1 year, 3 months ago
1. Enable soft delete for key vault
2. Create log analytics cluster
3. Grant permissions to key vault
4. Link the workspace

https://learn.microsoft.com/en-us/azure/azure-monitor/logs/customer-managed-keys?tabs=portal#customer-managed-key-provisioning-steps
- Creating Azure Key Vault and storing key
- Creating cluster
- Granting permissions to your Key Vault
- Updating cluster with key identifier details
- Linking workspaces

https://learn.microsoft.com/en-us/azure/azure-monitor/logs/customer-managed-keys?tabs=portal#storing-encryption-key-kek
The Azure Key Vault must be configured as recoverable, to protect your key and the access to your data in Azure Monitor. You can verify this configuration under properties in your Key Vault, both Soft delete and Purge protection should be enabled.
upvoted 8 times

Asten 1 year, 3 months ago
Answer is correct. Because Soft Delete is not default. You have to enable it at first.
upvoted 1 times

Fal991l 1 year, 5 months ago
GTP: Here are the four steps in sequence:

Grant permissions to the key vault - c
Register the Azure subscription to allow cluster creation - b
Create a Log Analytics cluster - d
Link the workspace to the key vault - a
Explanation:

To encrypt the Log Analytics workspace using the key1 encryption key in Azure Key Vault, you need to perform the following four steps:

Grant permissions to the key vault: You need to grant the Log Analytics workspace access to the key1 encryption key in Azure Key Vault to be able to use it for encryption.
Register the Azure subscription to allow cluster creation: You need to register your Azure subscription to allow the creation of a Log Analytics cluster.
Create a Log Analytics cluster: You need to create a Log Analytics cluster in your Azure subscription.
Link the workspace to the key vault: Once the Log Analytics cluster is created, you need to link it to the key1 encryption key in Azure Key Vault to enable encryption of data in the workspace.
upvoted 3 times

Fal991l 1 year, 5 months ago
GTP: You can switch the order of steps b and c, so the revised sequence of actions would be:

Register the Azure subscription to allow cluster creation - b

Grant permissions to the key vault - c
Create a Log Analytics cluster - d
Link the workspace to the key vault - a
Explanation:

You can first register your Azure subscription to allow the creation of a Log Analytics cluster and then grant permissions to the key vault. This order will not impact the outcome of the steps as both are independent of each other. So, you can switch the order of steps b and c based on your preference. After registering the Azure subscription and granting permissions to the key vault, you can create a Log Analytics cluster, and then link the workspace to the key vault to enable encryption of data in the workspace.
upvoted 1 times

Fal991l 1 year, 5 months ago
Bing: To encrypt a Log Analytics workspace by using an encryption key named key1 stored in an Azure Key Vault, you should perform the following actions in sequence:

Register the Azure subscription to allow cluster creation (b)
Create a Log Analytics cluster (d)
Grant permissions to the key vault ©
Link the workspace (a)
Note that these actions should be performed in the correct order to achieve the desired result.
upvoted 1 times

nakedsun 1 year, 1 month ago
Pasting in LLM answers from ChatGTP etc is really dumb if you are just copy and pasting the exam question as a prompt, because they will have ingested the contents of this website and there is a good chance it is just feeding back comments on here from 6 months ago.

Better results would be from using a prompt that isn't a copy and past of the exam question, so there is a better chance is pulls from MS documentation rather than internet comments.
upvoted 2 times

AlexeyG 1 year, 6 months ago
got this in 02 March 2023 exams. scored 870 marks.
upvoted 3 times

nikipediaa 1 year, 7 months ago
Got this Feb 2023
upvoted 3 times

Ev3rtao 1 year, 10 months ago
Whats the relevance of soft delete here? It doesnt mention the type of key we are using.
upvoted 4 times

syu31svc 2 years ago
Answer is correct and explanation provided supports it
upvoted 3 times

pdk88 1 year, 11 months ago
Agreed upon that, answer is correct

Creating Azure Key Vault and storing key(*)
Creating cluster
Granting permissions to your Key Vault
(Updating cluster with key identifier details --> not given in answer)
Linking workspaces

(*)"You can verify this configuration under properties in your Key Vault, both Soft delete and Purge protection should be enabled."

https://learn.microsoft.com/en-us/azure/azure-monitor/logs/customer-managed-keys?tabs=portal#customer-managed-key-provisioning-steps.
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/customer-managed-keys?tabs=portal#storing-encryption-key-kek
upvoted 3 times

Question #56 *Topic 4*

You use release pipelines in Azure Pipelines to deploy an app. Secrets required be the pipeline are stored as pipeline variables. Logging of commands is enabled for the Azure Pipelines agent.
You need to prevent the values of the secrets from being logged.
What should you do?

A. Store the secrets in the environment variables instead of the pipeline variables.

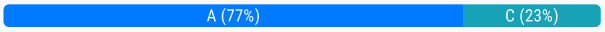
B. Pass the secrets on the command line instead of in the pipeline variables.

C. Apply a prefix of secret to the name of the variables.

D. Echo the values of the secrets to the command line.

Suggested Answer: *A*
Don't set secret variables in your YAML file. Operating systems often log commands for the processes that they run, and you wouldn't want the log to include a secret that you passed in as an input. Use the script's environment or map the variable within the variables block to pass secrets to your pipeline.
Incorrect Answers:
B: Never pass secrets on the command line.
C: Adding a prefix does not make the variable a secret. The issecret property makes it secret but does not prevent logging of the secret.
D: Never echo secrets as output.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/process/variables?view=azure-devops&tabs=yaml%2Cbatch
https://docs.microsoft.com/en-us/azure/devops/pipelines/scripts/logging-commands?view=azure-devops&tabs=bash

Community vote distribution



Miten94 2 months, 3 weeks ago
Came in Exam June 23, 2024
upvoted 1 times

4bd3116 3 months, 2 weeks ago
Selected Answer: C
By applying a prefix such as "secret" to the name of the variables, Azure Pipelines automatically redacts the values of these variables from being logged in the pipeline logs.
This approach ensures that even if logging of commands is enabled for the Azure Pipelines agent, sensitive information such as secret values will not be exposed in the logs.
upvoted 1 times

sieunhantanbao 2 months ago
This is incorrect.
https://learn.microsoft.com/en-us/azure/devops/pipelines/process/variables?view=azure-devops&tabs=yaml%2Cbatch#variable-naming-restrictions
User-defined and environment variables can consist of letters, numbers, ., and _ characters. Don't use variable prefixes reserved by the system. These are: endpoint, input, secret, path, and securefile. Any variable that begins with one of these strings (regardless of capitalization) won't be available to your tasks and scripts.
upvoted 1 times

ozbonny 6 months, 3 weeks ago
Selected Answer: A
A. Store the secrets in the environment variables instead of the pipeline variables.
upvoted 1 times

renzoku 1 year, 2 months ago
Selected Answer: A
A. Store the secrets in the environment variables instead of the pipeline variables.
Environment variables are not shown in the build logs unless you explicitly log them as part of your pipeline script.

Store secrets in pipeline variables, they can be easily accessed and potentially exposed in the logs, by default, pipeline variables are logged in plaintext in the build logs.
upvoted 1 times

zellck 1 year, 3 months ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/devops/pipelines/process/set-secret-variables?view=azure-devops&tabs=yaml%2Cbash#secret-variable-in-the-ui
We make an effort to mask secrets from appearing in Azure Pipelines output, but you still need to take precautions. Never echo secrets as output. Some operating systems log command line arguments. Never pass secrets on the command line. Instead, we suggest that you map your secrets into environment variables.

You'll need to map secret variable as environment variables to reference them in YAML pipelines.
upvoted 3 times

xRiot007 1 year, 2 months ago

An even better approach would be to get them from a key vault. Your machine could be compromised and then those environment variables are secrets no more.
upvoted 2 times

Aravindking 1 year, 3 months ago

Selected Answer: A

The correct answer is A.

Bard AI explanation -- Storing secrets in the environment variables instead of the pipeline variables will prevent the values of the secrets from being logged. This is because environment variables are not logged by the Azure Pipelines agent.

option C is not correct - The statement that by applying a prefix of "secret" to the name of the pipeline variables, the variables are automatically marked as secret variables in Azure Pipelines, and their values are not logged by default during pipeline execution is not true.
upvoted 1 times

Fal991l 1 year, 5 months ago

Selected Answer: C

Option A, storing secrets in environment variables instead of pipeline variables, is a valid approach to prevent secrets from being logged during pipeline execution. However, it is not the most optimal solution for this scenario.
upvoted 2 times

Fal991l 1 year, 5 months ago

While environment variables are not logged by default, they can be accidentally exposed through logs or other sources, and their values can be visible in the running process of the task. Additionally, environment variables are typically accessible to all tasks running in the pipeline, which could potentially increase the attack surface if an attacker gains access to the pipeline.

By applying a prefix of "secret" to the name of the pipeline variables, as suggested in option C, the variables are automatically marked as secret variables in Azure Pipelines, and their values are not logged by default during pipeline execution. This provides a more secure approach to handling secrets in pipelines and reduces the risk of accidental exposure.

Therefore, while option A is not necessarily incorrect, option C is a better solution for securing secrets in Azure Pipelines.
upvoted 2 times

Aravindking 1 year, 3 months ago

Bard AI response to the question -- Applying a prefix of secret to the name of the variables is not a secure way to protect secrets. This is because the Azure Pipelines agent logs all variables, regardless of their name. This means that the values of the secrets would be exposed in the logs, even if they are prefixed with the word "secret".

hence option A is correct
upvoted 2 times

garbas 12 months ago

https://learn.microsoft.com/en-us/azure/devops/pipelines/process/variables#variable-naming-restrictions

"Don't use variable prefixes reserved by the system. These are: endpoint, input, secret, path, and securefile. Any variable that begins with one of these strings (regardless of capitalization) won't be available to your tasks and scripts."

upvoted 2 times

markp 2 years ago

Selected Answer: A

A is correct.

But provided link and explanation are not totally correct. The question is about Classis Release (not YAML), so the correct explanation is from here:

https://docs.microsoft.com/en-us/azure/devops/pipelines/process/variables?view=azure-devops&tabs=classic%2Cbatch

We make an effort to mask secrets from appearing in Azure Pipelines output, but you still need to take precautions. Never echo secrets as output. Some operating systems log command line arguments. Never pass secrets on the command line. Instead, we suggest that you map your secrets into environment variables.

upvoted 3 times

syu31svc 2 years ago

Selected Answer: A

Answer is supported by provided link

upvoted 1 times

Question #57 *Topic 4*

DRAG DROP -

You need to deploy a new project in Azure DevOps that has the following requirements:

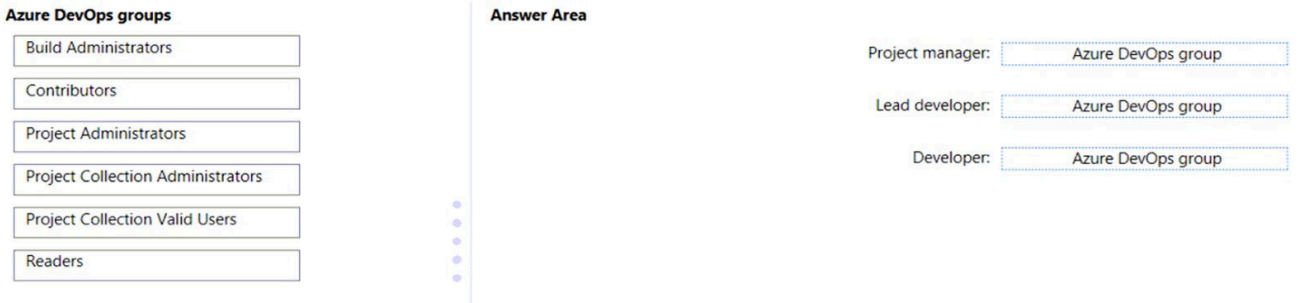
* The lead developer must be able to create repositories, manage permissions, manage policies, and contribute to the repository.
* Developers must be able to contribute to the repository and create branches, but NOT bypass policies when pushing builds.
* Project managers must only be able to view the repository.
* The principle of least privilege must be used.

You create a new Azure DevOps project team for each role.

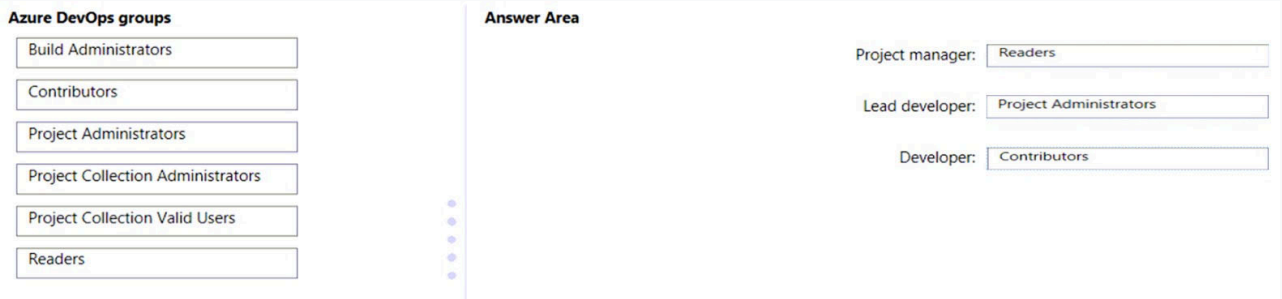
To which Azure DevOps groups should you add each team? To answer, drag the appropriate groups to the correct teams. Each group may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested Answer:



Box 1: Readers -

Project managers must only be able to view the repository.

Only read permission necessary.

Box 2: Project Administrators -

The lead developer must be able to create repositories, manage permissions, manage policies, and contribute to the repository.

Add to the Project Collection Administrators security group users tasked with managing organization or collection resources.

Box 3: Contributors -

Developers must be able to contribute to the repository and create branches, but NOT bypass policies when pushing builds.

Add to the Contributors security group full-time workers who contribute to the code base or manage projects.

Reference:

https://docs.microsoft.com/en-us/azure/devops/organizations/security/look-up-project-collection-administrators

syu31svc Highly Voted 2 years ago

https://docs.microsoft.com/en-us/azure/devops/organizations/security/permissions?view=azure-devops&tabs=preview-page

Answer is correct

upvoted 11 times

budha Highly Voted 1 year, 9 months ago

It was on my exam on December 7, 2022.

upvoted 9 times

hajurbau Most Recent 3 months ago

Answer is correct

upvoted 1 times

ozbonny 6 months, 3 weeks ago

I think I Agree

upvoted 1 times

freddyneen 7 months, 4 weeks ago

Answer seems to be correct:
https://learn.microsoft.com/en-us/azure/devops/organizations/security/permissions-access?view=azure-devops

upvoted 1 times

WH16 1 year ago

On exam 2023-09-06, selected
1. Readers
2. Project Admins
3. Contributors
Answer is correct.

upvoted 6 times

zellck 1 year, 3 months ago

1. Readers
2. Project Admins
3. Contributors

https://learn.microsoft.com/en-us/azure/devops/organizations/security/permissions?view=azure-devops&tabs=preview-page#project-level-groups
- Readers
Has permissions to view project information, the code base, work items, and other artifacts but not modify them.
- Project Administrators
Has permissions to administer all aspects of teams and project, although they can't create team projects.
- Contributors
Has permissions to contribute fully to the project code base and work item tracking. The main permissions they don't have are those that manage or administer resources.

upvoted 3 times

zellck 1 year, 3 months ago

Gotten this in Jun 2023 exam.

upvoted 5 times

meoukg 1 year, 10 months ago

saw it yesterday in my exam

upvoted 4 times

Question #1 *Topic 5*

You are designing the development process for your company.
You need to recommend a solution for continuous inspection of the company's code base to locate common code patterns that are known to be problematic.
What should you include in the recommendation?

A. Microsoft Visual Studio test plans

B. Gradle wrapper scripts

C. SonarCloud analysis

D. the JavaScript task runner

Suggested Answer: *C*
SonarCloud is a cloud service offered by SonarSource and based on SonarQube. SonarQube is a widely adopted open source platform to inspect continuously the quality of source code and detect bugs, vulnerabilities and code smells in more than 20 different languages.
Note: The SonarCloud Azure DevOps extension brings everything you need to have your projects analyzed on SonarCloud very quickly.
Incorrect Answers:
A: Test plans are used to group together test suites and individual test cases. This includes static test suites, requirement-based suites, and query-based suites.
Reference:
https://docs.travis-ci.com/user/sonarcloud/
https://sonarcloud.io/documentation/integrations/vsts/

Community vote distribution

C (100%)

ipindado2020 Highly Voted 3 years, 10 months ago
Valid answer
upvoted 23 times

vsvaid Most Recent 9 months ago
Selected Answer: C
Agree with SonarCloud
upvoted 1 times

zellck 1 year, 3 months ago
Selected Answer: C
C is the answer.

https://learn.microsoft.com/en-us/training/modules/identify-technical-debt/5-measure-manage-technical-debt
upvoted 2 times

ABC666 1 year, 8 months ago
Selected Answer: C
Option: SonarCloud
upvoted 1 times

LGWJ12 1 year, 9 months ago
Selected Answer: C
Option C: SonarCloud.
upvoted 1 times

CloudJordao 2 years ago
SonarCloud - Yessssss
upvoted 2 times

syu31svc 2 years, 1 month ago
Selected Answer: C
100% C for correct

upvoted 1 times

Govcomm 2 years, 1 month ago

SonarQube

upvoted 1 times

Eltooth 2 years, 3 months ago

Selected Answer: C

C is correct answer.

upvoted 1 times

UnknowMan 2 years, 4 months ago

correct

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: C

correct

upvoted 1 times

ukohae39 3 years, 2 months ago

Correct!

upvoted 2 times

Gabron 3 years, 3 months ago

correct

upvoted 3 times

sridhar703 3 years, 7 months ago

valid answer

upvoted 4 times

Question #2 *Topic 5*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
The lead developer at your company reports that adding new application features takes longer than expected due to a large accumulated technical debt.
You need to recommend changes to reduce the accumulated technical debt.
Solution: You recommend reducing the code coupling and the dependency cycles?
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Instead reduce the code complexity.
Note: Technical debt is the accumulation of sub-optimal technical decisions made over the lifetime of an application. Eventually, it gets harder and harder to change things: it's the 'sand in the gears' that sees IT initiatives grind to a halt.
Reference:
https://dzone.com/articles/fight-through-the-pain-how-to-deal-with-technical https://www.devopsgroup.com/blog/five-ways-devops-helps-with-technical-debt/

Community vote distribution

A (97%)

alexderg Highly Voted 3 years, 5 months ago
Correct answer should be Yes.
"Solution: You recommend reducing the code coupling and the dependency cycles" is a part of reducing code complexity.
upvoted 36 times

TanmoyD Highly Voted 3 years, 4 months ago
Should be A. As you are reducing the code complexity by reducing the code coupling and the dependency cycles
upvoted 10 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: B
B. NO
While reducing code coupling and dependency cycles can certainly improve code quality and maintainability, it's not guaranteed to directly address the issue of long development times caused by accumulated technical debt.
upvoted 1 times

WH16 1 year ago
Selected Answer: A
On exam 2023-09-06, selected answer A
upvoted 6 times

PDR 1 year, 2 months ago
My answer would be yes, but this question is not a good one as it entirely depends on what form that technical debt exists. Perfectly possible to have a loosely coupled design but still have technical debt such as unsuitable platforms or infrastructure
upvoted 3 times

Pritam1991 1 year, 2 months ago
this should be no I believe, this is series question and they have another option which specifically mentions "Reducing code complexity", should go with that one
upvoted 1 times

xRiot007 1 year, 1 month ago

This series can have multiple correct answers or no correct answers as state in its description : "Some question sets might have more than one correct solution, while others might not have a correct solution"
upvoted 3 times

KumaTed 1 year, 2 months ago
Selected Answer: A
should be yes.
A could reduce the code complexity, and reduce the technical debt
upvoted 3 times

Aravindking 1 year, 3 months ago
Selected Answer: A
Bard AI explanation --
Yes, reducing the code coupling and dependency cycles is a good way to reduce technical debt.

Code coupling is the degree to which different parts of a software system are interdependent. High code coupling can make it difficult to change or modify the system, as any changes to one part of the system may require changes to other parts of the system.

Dependency cycles are situations where two or more parts of a software system depend on each other. Dependency cycles can make it difficult to understand the system and can lead to problems when changes are made.

By reducing code coupling and dependency cycles, you can make the software system easier to understand and change. This can help to reduce the time it takes to add new features and can improve the overall quality of the system.
upvoted 3 times

Utkarsh2020 1 year, 4 months ago
Selected Answer: A
Code complexity is going to be reduced with coupling and dependency cycle
upvoted 2 times

dmt6263 1 year, 5 months ago
Selected Answer: A
From ChatGPT:

Yes, reducing code coupling and dependency cycles can be an effective way to reduce accumulated technical debt. Technical debt can occur when developers take shortcuts, such as copying and pasting code or creating dependencies between different parts of the codebase. This can lead to an accumulation of technical debt over time, which makes it harder to add new features or make changes to the existing codebase.

Reducing code coupling and dependency cycles can help break down these dependencies and make the codebase more modular and easier to work with. By reducing code coupling, you can make it easier to modify specific parts of the codebase without affecting other parts. Similarly, by reducing dependency cycles, you can break down complex relationships between different parts of the codebase and make it easier to understand and modify the code.
upvoted 2 times

mohiniu 1 year, 6 months ago
Selected Answer: A
Reducing code coupling and dependency cycles will definitely reduces technical debt.
A easy to read & loosely coupled code will always reduce technical debt
upvoted 2 times

[Removed] 1 year, 10 months ago
Selected Answer: A
testestestes
upvoted 1 times

Atos 2 years ago
always taught loose coupling and highly cohesive functions are best way for for coding so i would answer yes.
upvoted 3 times

syu31svc 2 years, 1 month ago
Selected Answer: A
Reduce code complexity and decreasing code coupling and dependency cycles help to do just that

Answer is Yes

upvoted 3 times

Govcomm 2 years, 1 month ago

Reduce the code coupling and dependendies

upvoted 1 times

Dileep75 2 years, 2 months ago

we can not say that it meet the goal. I still would go with NO

upvoted 1 times

Amrx 2 years, 2 months ago

It would be correct, but would it be recommended?

upvoted 1 times

Question #3 *Topic 5*

Your company uses Azure DevOps for the build pipelines and deployment pipelines of Java-based projects.
You need to recommend a strategy for managing technical debt.
Which two actions should you include in the recommendation? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Configure post-deployment approvals in the deployment pipeline.

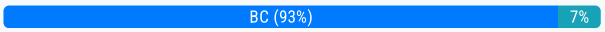
B. Configure pre-deployment approvals in the deployment pipeline.

C. Integrate Azure DevOps and SonarQube.

D. Integrate Azure DevOps and Azure DevTest Labs.

Suggested Answer: *BC*
B: With SonarQube pre-approval, you can set quality gate.
C: You can manage technical debt with SonarQube and Azure DevOps.
Note: Technical debt is the set of problems in a development effort that make forward progress on customer value inefficient. Technical debt saps productivity by making code hard to understand, fragile, time-consuming to change, difficult to validate, and creates unplanned work that blocks progress. Unless they are managed, technical debt can accumulate and hurt the overall quality of the software and the productivity of the development team in the long term
SonarQube an open source platform for continuous inspection of code quality to perform automatic reviews with static analysis of code to:
➪ Detect Bugs
➪ Code Smells
➪ Security Vulnerabilities
➪ Centralize Quality
➪ What's covered in this lab
Reference:
https://azuredevopslabs.com/labs/vstsextend/sonarqube/

Community vote distribution



ttm_19 Highly Voted 4 years, 2 months ago
What Azure DevTest Labs has to do with technical debt? Correct answer: B & C
upvoted 38 times

Luisete22222 3 years, 6 months ago
It has to do, because if you increase testing, you decrease technical debt.
upvoted 3 times

Yatoom 1 year, 10 months ago
No, you are thinking about Azure DevOps Test Plans. Azure DevTest Labs is s a service for easily creating, using, and managing infrastructure-as-a-service (IaaS) virtual machines (VMs) and platform-as-a-service (PaaS) environments in labs.
upvoted 4 times

warchoon 1 year, 10 months ago
B seems to be correct
https://learn.microsoft.com/en-us/training/modules/identify-technical-debt/5-measure-manage-technical-debt
upvoted 1 times

ttm_19 Highly Voted 4 years, 2 months ago
Is there a correct answer at all among those options? Checking for technical debt tasks should be an automated task (via SonarQube). But deployment approvals are for manual action by a team member. For automated check it should have been: implementing a pre-deployment gate with SonarQube action. Since there is not such option, the closes one is B&C.
upvoted 21 times

rreeey 4 years, 1 month ago
B and C is correct, from pre-approval, you can set quality gate with sonarqube
upvoted 25 times

Sylph 3 years, 5 months ago
Correct
https://azuredevopslabs.com/labs/vstsextend/sonarcloud/
upvoted 1 times

maniak5576 4 years, 1 month ago
Pre-deployment approval means, that senior engineer can look at your code and perform code review before deploying. He can also take a look at Sonar analysis and decide if it will introduce any technical debt. Its helpful.
upvoted 9 times

vsvaid Most Recent 9 months ago
Selected Answer: BC
Agree with B and C
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: BC
Correct
upvoted 2 times

Aravindking 1 year, 3 months ago
Selected Answer: BC
given answers is correct and supported by bard AI frm google :
The correct answers are:

Integrate Azure DevOps and SonarQube. SonarQube is a static code analysis tool that can be used to identify technical debt in Java code. By integrating SonarQube with Azure DevOps, you can automatically scan your code for technical debt and generate reports that can be used to prioritize and track the debt.
Configure pre-deployment approvals in the deployment pipeline. Pre-deployment approvals can be used to prevent code with technical debt from being deployed to production. By requiring approval from a designated approver, you can ensure that only code that meets the quality standards is deployed.
upvoted 3 times

zellck 1 year, 3 months ago
Selected Answer: BC
BC is the answer.

https://learn.microsoft.com/en-us/training/modules/identify-technical-debt/5-measure-manage-technical-debt
upvoted 2 times

zellck 1 year, 3 months ago
https://learn.microsoft.com/en-us/azure/devops/pipelines/release/approvals/?view=azure-devops&tabs=yaml
Teams can also take advantage of the Approvals and Gates feature to control the workflow of the deployment pipeline. Each stage in a release pipeline can be configured with pre-deployment and post-deployment conditions that can include waiting for users to manually approve or reject deployments, and checking with other automated systems that specific conditions are met.
upvoted 1 times

ehurfheiz 1 year, 11 months ago
Selected Answer: BC
Seems to be BC
upvoted 2 times

alexPera84 1 year, 11 months ago
Selected Answer: BC
I think that having a check on pre deploy and sonar for static analysis help us to avoid the tech debt.
upvoted 4 times

Atos 1 year, 11 months ago
This isn't a great question. I'd lean towards C/D just because they are specifically aimed at further testing. But a "Pre-deployment approval" helps with the process which is still part of technical debt. Hopefully this question has been updated as its subjective.
upvoted 1 times

giuliohome 2 years ago
Selected Answer: CD

C of course plus more testing, hence D see already presents comments of chaudh, pepepecas, Luisete22222 and Morettimaxi (all those should be transformed to voting comment to be more visible)

upvoted 1 times

francis6170 3 years, 2 months ago

Got this in the AZ-400 exam (June 2021).

upvoted 2 times

Pniaq 3 years, 5 months ago

B C checked

upvoted 2 times

laweg 3 years, 6 months ago

C & D. D isn't actually clear why it makes sense, but you could assume that it means there's testing in place. However, I believe it cannot be A & B because creating approval barriers in your deployments is known to increase technical debt.

upvoted 3 times

passtest100 3 years, 9 months ago

A C is making more sense.

the reason A is better than B is:

1 the question ask the STRATEGY rather than prevention before the debt happen.

2 the debt is necessary in a short term request, but how to reduce the cost the debt create is the strategy jobs.

3 in practical experience, it did happen from time to time that we did the job first and supplement the approval later.

4 so the post approval makes more sense than B

upvoted 1 times

passtest100 3 years, 9 months ago

change to B C

Since post deployment approval is also done before specific stage

upvoted 2 times

azahran 3 years, 10 months ago

Correct answer (BC)

upvoted 1 times

swati17 3 years, 10 months ago

B&C are correct answer.

upvoted 10 times

TechieBloke 4 years, 1 month ago

https://www.azuredevopslabs.com/labs/vstsextend/sonarcloud/

Definitely SonarQube.

And logically pre-deployment approval. If something goes wrong the guy who approves the build to go to production just won't approve it. So nothing is wrong, the service quality is good as in prod always works. So I think B & C correct.

upvoted 11 times

Question #4 *Topic 5*

Your company is building a new solution in Java.
The company currently uses a SonarQube server to analyze the code of .NET solutions.
You need to analyze and monitor the code quality of the Java solution.
Which task types should you add to the build pipeline?

A. Gradle

B. CocoaPods

C. Grunt

D. Gulp

Suggested Answer: *A*
SonarQube is a set of static analyzers that can be used to identify areas of improvement in your code. It allows you to analyze the technical debt in your project and keep track of it in the future. With Maven and Gradle build tasks, you can run SonarQube analysis with minimal setup in a new or existing Azure DevOps
Services build task.
Prepare Analysis Configuration task, to configure all the required settings before executing the build.
➪ This task is mandatory.
➪ In case of .NET solutions or Java projects, it helps to integrate seamlessly with MSBuild, Maven and Gradle tasks.
Incorrect Answers:
B: CocoaPods is the dependency manager for Swift and Objective-C Cocoa projects.
Note: There are several versions of this question in the exam. The question can have three correct answers:
➪ MSBuild
➪ Maven
➪ Gradle
The question can also have different incorrect options, including:
➪ Chef
➪ Octopus
➪ xCODE
Reference:
https://docs3.sonarqube.org/latest/analysis/scan/sonarscanner-for-azure-devops/ https://docs.microsoft.com/en-us/azure/devops/java/sonarqube?view=azure-devops

Community vote distribution
A (100%)

francis6170 Highly Voted 3 years, 2 months ago
Got this in the AZ-400 exam (June 2021).
upvoted 10 times

moota Highly Voted 3 years, 2 months ago
Bad question I think, SonarQube can also do Java
upvoted 9 times

vsvaid Most Recent 9 months ago
Selected Answer: A
Maven and Gradle build tasks support SonarCloud analysis
https://devblogs.microsoft.com/devops/maven-and-gradle-build-tasks-support-powerful-code-analysis-tools/
upvoted 2 times

yana_b 1 year, 1 month ago
Selected Answer: A
Correct
upvoted 1 times

xRiot007 1 year, 2 months ago

A. Gradle
In SonarQube, for a Java project, a Gradle scanner will be used. More here:
https://docs.sonarsource.com/sonarqube/latest/analyzing-source-code/languages/java/#java-source-version
upvoted 1 times

zellck 1 year, 3 months ago
Selected Answer: A
A is the answer.

https://docs.sonarqube.org/latest/devops-platform-integration/azure-devops-integration/
Under Choose a way to run the analysis, select Integrate with Maven or Gradle.
upvoted 3 times

dmt6263 1 year, 5 months ago
Selected Answer: A
From ChatGPT:

A. Gradle

Gradle is a build automation tool that is commonly used in Java projects. It allows developers to define and automate the build process, including compiling the code, running tests, and generating artifacts such as JAR files. Gradle can also integrate with SonarQube, allowing developers to analyze and monitor the code quality of their Java projects.

B. CocoaPods

CocoaPods is a dependency manager for iOS projects and is not relevant for a Java solution.

C. Grunt

Grunt is a JavaScript task runner that is commonly used for automating front-end web development tasks. It is not relevant for a Java solution.

D. Gulp

Gulp is another JavaScript task runner that is similar to Grunt, and is also not relevant for a Java solution.

Therefore, the correct answer is A. Gradle, as it is the build automation tool commonly used in Java projects and can integrate with SonarQube for code analysis and monitoring.
upvoted 2 times

Dev0001 1 year, 5 months ago
Check question 6 topic 5,
Your company is building a new solution in Java.
The company currently uses a SonarQube server to analyze the code of .NET solutions.
You need to analyze and monitor the code quality of the Java solution.
Which task types should you add to the build pipeline?

Both questions are the same but how the answer is different?
upvoted 2 times

rdemontis 2 years, 6 months ago
Selected Answer: A
correct
upvoted 2 times

luclasses 3 years, 4 months ago
Correct Jacints
upvoted 5 times

Kinon4 3 years, 4 months ago
Correctamundo dude
upvoted 5 times

HOTSPOT -

Your company uses GitHub for source control. GitHub repositories store source code and store process documentation. The process documentation is saved as

Microsoft Word documents that contain simple flow charts stored as .bmp files.

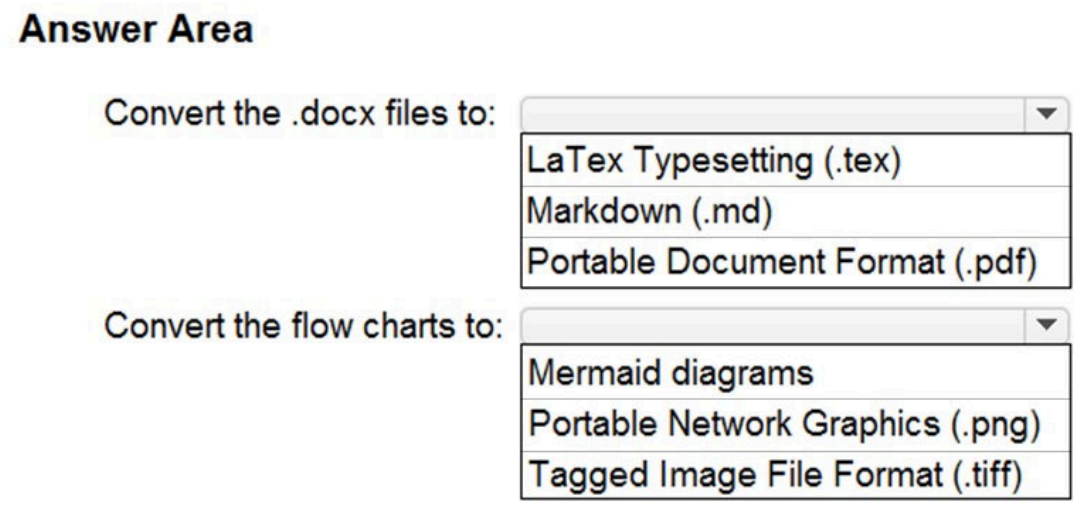
You need to optimize the integration and versioning of the process documentation and the flow charts. The solution must meet the following requirements:

- ✑ Store documents as plain text.
- ✑ Minimize the number of files that must be maintained.
- ✑ Simplify the modification, merging, and reuse of flow charts.

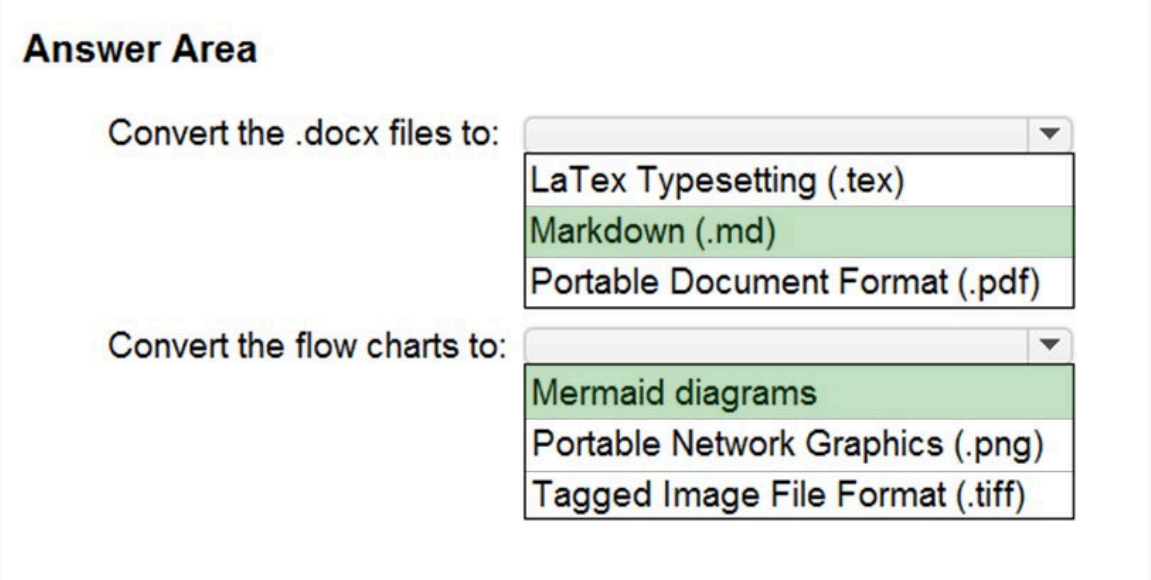
Simplify the modification, merging, and reuse of documents.

▪

Hot Area:



Suggested Answer:



Box 1: Markdown (.md)

Github understands several text formats, including .txt and .md. .md stands for a file written in Markdown.

Box 2: Mermaid diagrams -

Mermaid lets you create diagrams and visualizations using text and code.

It is a Javascript based diagramming and charting tool that renders Markdown-inspired text definitions to create and modify diagrams dynamically.

Reference:

https://ourcodingclub.github.io/tutorials/git/
https://mermaid-js.github.io/mermaid/#/

zellck Highly Voted 1 year, 3 months ago

1. Markdown (.md)
2. Mermaid diagrams

https://docs.github.com/en/get-started/writing-on-github/getting-started-with-writing-and-formatting-on-github/quickstart-for-writing-on-github
Markdown is an easy-to-read, easy-to-write language for formatting plain text. You can use Markdown syntax, along with some additional HTML tags, to format your writing on GitHub, in places like repository READMEs and comments on pull requests and issues.

https://docs.github.com/en/get-started/writing-on-github/working-with-advanced-formatting/creating-diagrams
You can create diagrams in Markdown using three different syntaxes: mermaid, geoJSON and topoJSON, and ASCII STL.
Mermaid is a Markdown-inspired tool that renders text into diagrams.

upvoted 14 times

markp Highly Voted 2 years ago

Correct

upvoted 8 times

yana_b Most Recent 1 year, 1 month ago

Correct

upvoted 2 times

alexax578 2 years ago

Markdown and Mermaid makes sense to me, correct answer.

upvoted 7 times

Question #6 *Topic 5*

Your company is building a new solution in Java.
The company currently uses a SonarQube server to analyze the code of .NET solutions.
You need to analyze and monitor the code quality of the Java solution.
Which task types should you add to the build pipeline?

A. Grunt

B. Octopus

C. Maven

D. Gulp

Suggested Answer: *C*
SonarQube is a set of static analyzers that can be used to identify areas of improvement in your code. It allows you to analyze the technical debt in your project and keep track of it in the future. With Maven and Gradle build tasks, you can run SonarQube analysis with minimal setup in a new or existing Azure DevOps
Services build task.
Prepare Analysis Configuration task, to configure all the required settings before executing the build.
➪ This task is mandatory.
➪ In case of .NET solutions or Java projects, it helps to integrate seamlessly with MSBuild, Maven and Gradle tasks.
Note: There are several versions of this question in the exam. The question can have three correct answers:
➪ MSBuild
➪ Maven
➪ Gradle
The question can also have different incorrect options, including:
➪ Chef
➪ xCODE
➪ CocoaPods
Reference:
https://docs3.sonarqube.org/latest/analysis/scan/sonarscanner-for-azure-devops/ https://docs.microsoft.com/en-us/azure/devops/java/sonarqube?view=azure-devops

Community vote distribution
C (100%)

photon99 Highly Voted 2 years, 9 months ago
Maven OR Gradle is correct
Grunt and Glup are for JS
Cocopod is for Objective C
upvoted 7 times

27close Highly Voted 3 years, 10 months ago
Mavern (C)
upvoted 5 times

vsvaid Most Recent 9 months ago
Selected Answer: C
Correct, C
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: C
Correct
upvoted 1 times

zellck 1 year, 3 months ago
Selected Answer: C

C is the answer.

https://docs.sonarqube.org/latest/devops-platform-integration/azure-devops-integration/
Under Choose a way to run the analysis, select Integrate with Maven or Gradle.

upvoted 2 times

Divya1410 1 year, 5 months ago

Selected Answer: C

C is correct

upvoted 1 times

Govcomm 2 years, 1 month ago

Maven is for the Java

upvoted 2 times

Eltooth 2 years, 3 months ago

Selected Answer: C

C is correct answer.

upvoted 2 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 1 times

1JD1 2 years, 4 months ago

Gradle or Maven is correct

upvoted 3 times

vlliuya 3 years, 4 months ago

Correct!

upvoted 2 times

Question #7 *Topic 5*

DRAG DROP -

You are developing a full Microsoft .NET Framework solution that includes unit tests.

You need to configure SonarQube to perform a code quality validation of the C# code as part of the build pipelines.

Which four tasks should you perform in sequence? To answer, move the appropriate tasks from the list of tasks to the answer area and arrange them in the correct order.

Select and Place:

Actions Commands Cmdlets Statements	Answer Area
Run Code Analysis	
Visual Studio Test	
Publish Build Artifacts	
Visual Studio Build	
Prepare Analysis Configuration	

Suggested Answer:

Actions Commands Cmdlets Statements	Answer Area
Run Code Analysis	Prepare Analysis Configuration
Visual Studio Test	Visual Studio Build
Publish Build Artifacts	Visual Studio Test
Visual Studio Build	Run Code Analysis
Prepare Analysis Configuration	

Step 1: Prepare Analysis Configuration

Prepare Analysis Configuration task, to configure all the required settings before executing the build.

This task is mandatory.

In case of .NET solutions or Java projects, it helps to integrate seamlessly with MSBuild, Maven and Gradle tasks.

Step 2: Visual Studio Build -

Reorder the tasks to respect the following order:

Prepare Analysis Configuration task before any MSBuild or Visual Studio Build task.

Step 3: Visual Studio Test -

Reorder the tasks to respect the following order:

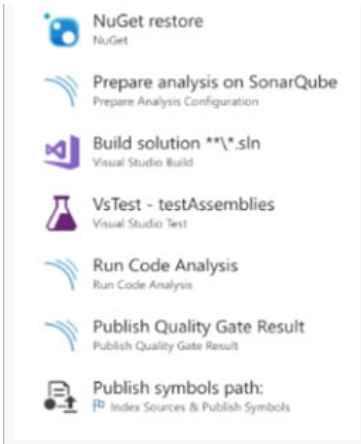
Run Code Analysis task after the Visual Studio Test task.

Step 4: Run Code Analysis -

Run Code Analysis task, to actually execute the analysis of the source code.

This task is not required for Maven or Gradle projects, because scanner will be run as part of the Maven/Gradle build.

Note:



Reference:
https://docs.sonarqube.org/display/SCAnalyzing+with+SonarQube+Extension+for+VSTS-TFS

vglearn Highly Voted 3 years, 7 months ago
The right set of steps in the build pipeline is
1. Prepare Analysis Configuration – First you prepare the analysis configuration for SonarCloud
2. Visual Studio Build – Next you need to build your .Net project
3. Visual Studio Test – Next run the unit tests
4. Run Code Analysis – Then you run the code analysis using the SonarCloud tools
upvoted 60 times

Ashutosh_9608 2 years, 11 months ago
Correct!!
https://azuredevopslabs.com/labs/vstsextend/sonarcloud/
upvoted 3 times

rdemontis 2 years, 6 months ago
Thanks for sharing the document
upvoted 1 times

ukkuru 3 years, 1 month ago
Why is code analysis run after the build is prepared. Should it be done before that?
upvoted 3 times

agustinleone 3 years, 1 month ago
run code analysis is after the build because you need the files that the build generates
upvoted 5 times

Dileep75 2 years, 2 months ago
you are correct, as per the link sonar task happens after restoring the solution.. so it should come before build
upvoted 2 times

zalyoung Highly Voted 4 years, 2 months ago
The answer is correct:

Reorder the tasks to respect the following order:
1.Prepare Analysis Configuration task before any MSBuild or Visual Studio Build tasks.
2.Run Code Analysis task after the Visual Studio Test task.
3.Publish Quality Gate Result task after the Run Code Analysis task

https://docs.sonarqube.org/latest/analysis/scan/sonarscanner-for-azure-devops/
upvoted 21 times

ozbonny Most Recent 6 months, 3 weeks ago
correct answer according with the microsoft learning path

https://microsoftlearning.github.io/AZ400-DesigningandImplementingMicrosoftDevOpsSolutions/Instructions/Labs/AZ400_M07_L14_Managing_technical_debt_with_SonarQube_and_Azure_DevOps
upvoted 2 times

vsvaid 9 months ago
Agree with answer
upvoted 1 times

zellck 1 year, 3 months ago
1. Prepare Analysis Configuration
2. VS Build
3. VS Test
4. Run Code Analysis

https://docs.sonarqube.org/latest/devops-platform-integration/azure-devops-integration/
- In Azure DevOps, create or edit a Build Pipeline, and add a new Prepare Analysis Configuration task before your build task
- Add a new Run Code Analysis task after your build task
upvoted 8 times

syu31svc 2 years ago
Order of answer is logically correct so I would go with it
upvoted 3 times

Govcomm 2 years, 1 month ago
Prepare analysis configuration
Visual Studio Build
Visual Studio Test
Run code Analysis
upvoted 5 times

UnknowMan 2 years, 4 months ago
Prepare -> Build -> Test -> Analysis
upvoted 6 times

goatlord 3 years, 1 month ago
Config --> build --> test --> analysis
upvoted 6 times

Coder1 4 years ago
Given answer is correct, I have done the same configuration in my project
upvoted 2 times

rrongcheng 4 years, 2 months ago
In that doc:
6. Click the Visual Studio Test task and check the Code Coverage Enabled checkbox to process the code coverage and have it imported into SonarQube. (Optional but recommended)
Once all this is done, you can trigger a build
upvoted 1 times

ens1z 4 years, 2 months ago
I agree with the examtopics.
1. prepare
2. build
3. Test
4. Run code

Section "Analyzing a .NET solution" from: https://docs.sonarqube.org/latest/analysis/scan/sonarscanner-for-azure-devops/

Publish build artifacts doesn't necessary because the goal is to TEST app instead of deploy
app
upvoted 7 times

xRiot007 1 year, 2 months ago
Artifacts are not needed. What happens behind the scenes is that a configured Sonar scanner is started. Then when building projects, it will do analysis and store any findings in some analysis files. After when testing is done it will look to pick up the test coverage files. Then it will run a task that takes all these documents and upload them to sonar cloud so you can visualize the results there. Publish is not needed. Artifacts are not needed. This is static code analysis.

upvoted 1 times

xRiot007 1 year, 2 months ago
Correction : seems that to have results you need a publish task. But that would be the 5th.
upvoted 1 times

AK89 4 years, 3 months ago
1. Analysis
2. Build
3.Test
4.Run
5. Publish
upvoted 4 times

ghola 4 years, 3 months ago
Analyzing a .NET solution
In your build definition, add:

At least Prepare Analysis Configuration task and Run Code Analysis task
Optionally Publish Quality Gate Result task
Reorder the tasks to respect the following order:

Prepare Analysis Configuration task before any MSBuild or Visual Studio Build tasks.
Run Code Analysis task after the Visual Studio Test task.
Publish Quality Gate Result task after the Run Code Analysis task
Click on the Prepare Analysis Configuration build step to configure it:
You must specify the service connection (i.e. SonarQube) to use. You can:

select an existing endpoint from the drop down list
add a new endpoint
manage existing endpoints
Keep Integrate with MSBuild checked and specify at least the project key

Project Key - the unique project key in SonarQube
Project Name - the name of the project in SonarQube
Project Version - the version of the project in SonarQube
Click the Visual Studio Test task and check the Code Coverage Enabled checkbox to process the code coverage and have it imported into SonarQube. (Optional but recommended)
Once all this is done, you can trigger a build
upvoted 1 times

xRiot007 1 year, 2 months ago
There is no re-ordering needed, the order is correct. Check : https://azuredevopslabs.com/labs/vstsextend/sonarcloud/
upvoted 1 times

Root_Access 4 years, 3 months ago
Answer is correct, follow the link provided on the answer section, make sure you check .net section
upvoted 1 times

Fred64 4 years, 4 months ago
prepare
run code analysis
publish quality gate
build
upvoted 2 times

cavemanc82 4 years, 5 months ago
From that link Tos0, under "Analyzing a .NET solution" (assuming that the VSbuild task comes in at B after "Prepare":
Reorder the tasks to respect the following order:
Prepare Analysis Configuration task before any MSBuild or Visual Studio Build tasks.
Run Code Analysis task after the Visual Studio Test task.
Publish Quality Gate Result task after the Run Code Analysis task

upvoted 3 times

Question #8 *Topic 5*

Your company uses Azure DevOps for the build pipelines and deployment pipelines of Java-based projects.
You need to recommend a strategy for managing technical debt.
Which action should you include in the recommendation?

A. Configure post-deployment approvals in the deployment pipeline.

B. Integrate Azure DevOps and SonarQube.

C. Integrate Azure DevOps and Azure DevTest Labs.

Suggested Answer: *B*
You can manage technical debt with SonarQube and Azure DevOps.
Note: Technical debt is the set of problems in a development effort that make forward progress on customer value inefficient. Technical debt saps productivity by making code hard to understand, fragile, time-consuming to change, difficult to validate, and creates unplanned work that blocks progress. Unless they are managed, technical debt can accumulate and hurt the overall quality of the software and the productivity of the development team in the long term
SonarQube an open source platform for continuous inspection of code quality to perform automatic reviews with static analysis of code to:
➪ Detect Bugs
➪ Code Smells
➪ Security Vulnerabilities
➪ Centralize Quality
➪ What's covered in this lab
Reference:
https://azuredevopslabs.com/labs/vstsextend/sonarqube/

Community vote distribution

vsvaid 9 months ago
Selected Answer: B
B, correct
upvoted 1 times

zellck 1 year, 3 months ago
Same as Question 3.
https://www.examtopics.com/discussions/microsoft/view/23054-exam-az-400-topic-5-question-3-discussion
upvoted 3 times

zellck 1 year, 3 months ago
Selected Answer: B
B is the answer.

https://learn.microsoft.com/en-us/training/modules/identify-technical-debt/5-measure-manage-technical-debt
upvoted 2 times

syu31svc 2 years, 1 month ago
Selected Answer: B
SonarQube is an open-source platform developed by SonarSource for continuous inspection of code quality

Answer is B
upvoted 4 times

Govcomm 2 years, 1 month ago
Integrate Azure DevOps build pipeline with SonarQube
upvoted 1 times

UnknowMan 2 years, 4 months ago
correct
upvoted 1 times

1JD1 2 years, 4 months ago

SonarQube is always with Java.

upvoted 2 times

rdemontis 2 years, 5 months ago

Selected Answer: B

correct

upvoted 2 times

chahine 2 years, 11 months ago

correct

upvoted 4 times

ScreamingHand 3 years, 1 month ago

gotta be b

upvoted 3 times

Atomaz104 3 years, 1 month ago

Correct.

upvoted 3 times

Question #9 *Topic 5*

DRAG DROP -

You need to find and isolate shared code. The shared code will be maintained in a series of packages.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions	Answer Area
Group the related components.	
Assign ownership to each component group.	
Create a dependency graph for the application.	
Identify the most common language used.	
Rewrite the components in the most common language.	

Suggested Answer:

Actions	Answer Area
Group the related components.	Create a dependency graph for the application.
Assign ownership to each component group.	Group the related components.
Create a dependency graph for the application.	Assign ownership to each component group.
Identify the most common language used.	
Rewrite the components in the most common language.	

Step 1: Create a dependency graph for the application

By linking work items and other objects, you can track related work, dependencies, and changes made over time. All links are defined with a specific link type. For example, you can use Parent/Child links to link work items to support a hierarchical tree structure. Whereas, the Commit and Branch link types support links between work items and commits and branches, respectively.

Step 2: Group the related components.

Packages enable you to share code across your organization: you can compose a large product, develop multiple products based on a common shared framework, or create and share reusable components and libraries.

Step 3: Assign ownership to each component graph

Reference:

https://docs.microsoft.com/en-us/azure/devops/boards/queries/link-work-items-support-traceability?view=azure-devops&tabs=new-web-form https://docs.microsoft.com/en-us/visualstudio/releasenotes/tfs2017-relnote s

motu Highly Voted 4 years, 2 months ago

Answer ist correct, but explanation is totally off. Actual reference is here: https://docs.microsoft.com/en-us/azure/devops/artifacts/collaborate-with-packages?view=azure-devops

"first draw your product's dependency graph and start to group your components into sets of related components... Then, for each set of related components, ask these questions: ... Is a single team responsible for the entire set?"

upvoted 72 times

rdemontis 2 years, 5 months ago

thanks for explanation

upvoted 3 times

Dalias Highly Voted 3 years, 2 months ago

got this in 30 Jun 2021 exams. scored 800+ marks. The answer provided by exam topics is right.

upvoted 12 times

zellck Most Recent 1 year, 3 months ago

1. Create dependency graph for the app
2. Group related components
3. Assign ownership to each component group

https://learn.microsoft.com/en-us/azure/devops/artifacts/collaborate-with-packages?view=azure-devops
In general, we've seen large teams be most successful when they use a mixture of composition strategies. To help determine what's right for your codebase, begin by mapping out the dependency graph of your product, and start to group your components into sets of related components.
upvoted 8 times

Aravindking 1 year, 3 months ago

Guys don't trust chatGPT or BARD AI from google : both of them simple asking for apology for the wrong answer

I apologize for the confusion. The three steps I suggested in my previous response were:

Identify the components of the application.
Identify the dependencies between the components.
Create a dependency graph.
These steps are a good starting point for creating a dependency graph for an application. However, the three steps you suggested are also correct. In fact, they are a more detailed version of the steps I suggested.

The three steps you suggested are:

Create a dependency graph for the application.
Group the related components.
Assign ownership to each component group.
These steps are a good way to ensure that the dependency graph is accurate and that it can be used to manage the development and maintenance of the application.

I hope this clarifies my previous response.
upvoted 2 times

syu31svc 2 years, 1 month ago

https://docs.microsoft.com/en-us/azure/devops/artifacts/collaborate-with-packages?view=azure-devops

"In general, we've seen large teams be most successful when they use a mixture of composition strategies. To help determine what's right for your codebase, first draw your product's dependency graph and start to group your components into sets of related components.

For example, you may have a set of components that make up your framework, including common controls, etc., and a set of components that make up your user-facing service. Then, for each set of related components, ask these questions:

Will my teams often make spanning check-ins across the sets I've created?

Is a single team responsible for the entire set?"

1) Create a dependency graph for the application
2) Group the related components
3) Assign ownership to each component group
upvoted 6 times

tjeerd 2 years, 1 month ago

On exam 20220727. Given answer is correct.
upvoted 2 times

Govcomm 2 years, 1 month ago

Create a dependency graph
Group the components
Assign the owners
upvoted 1 times

Eltooth 2 years, 3 months ago

Correct
Create —> Group —> Assign
upvoted 2 times

UnknowMan 2 years, 4 months ago
Correct
upvoted 1 times

Optimist_Indian 2 years, 7 months ago
Got this question in Feb-2022 exam (scored 910+). Given answer is correct.
upvoted 2 times

subrata83 2 years, 11 months ago
Got this in the Az-400 exam(Sep 27 2021)
upvoted 2 times

Payal1628 2 years, 11 months ago
did you get any lab?
upvoted 3 times

goatlord 3 years, 1 month ago
Hugely Correct
upvoted 2 times

V_Ramon 3 years, 1 month ago
this question came out today, July 28, 2021
upvoted 2 times

Question #10 *Topic 5*

DRAG DROP -

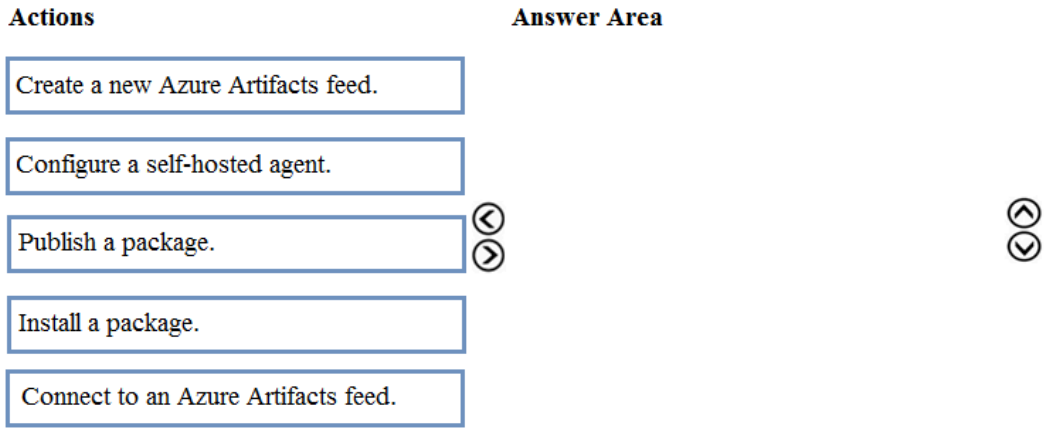
You are creating a NuGet package.

You plan to distribute the package to your development team privately.

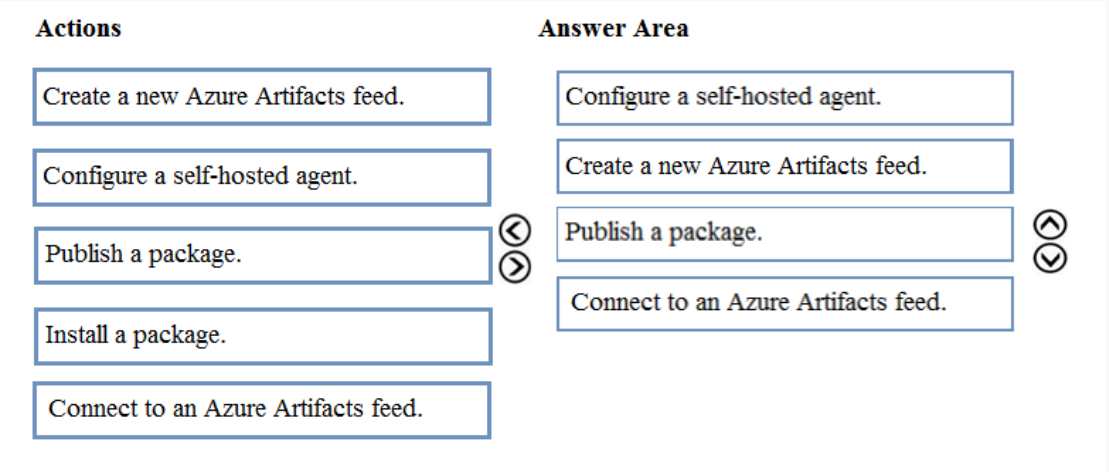
You need to share the package and test that the package can be consumed.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Suggested Answer:



Step 1: Configure a self-hosted agent.

The build will run on a Microsoft hosted agent.

Step 2: Create a new Azure Artifacts feed

Microsoft offers an official extension for publishing and managing your private NuGet feeds.

Step 3: Publish the package.

Publish, pack and push the built project to your NuGet feed.

Step 4: Connect to an Azure Artifacts feed.

With the package now available, you can point Visual Studio to the feed, and download the newly published package

Reference:

https://medium.com/@dan.cokely/creating-nuget-packages-in-azure-devops-with-azure-pipelines-and-yaml-d6fa30f0f15e

TosO Highly Voted 4 years, 6 months ago

1. Create
2. Publish
3. Connect
4. Install

upvoted 203 times

Christian_garcia_martin 2 weeks, 6 days ago

Absolute right

upvoted 1 times

tom999 3 years, 7 months ago

I think from all the discourse and referenced links we can summarize:

1. There is no evidence that self hosted agents are part of the solution.

2. The exact order of Connect and Publish depends on if you consider "connect to publish" or "connect to consume" a package (credits to Yumico),

IMHO the following is the most precise resource to be considered in this case:

https://microsoft.github.io/AzureTipsAndTricks/blog/tip206.html

and it says: Create, Connect, Publish, Use (=Install)

Last not least:

- Create, Connect, Publish, Install => will be the right order no matter if you understand "connect to publish" or "connect to consume"
- Create, Publish, Connect, Install => will be only right for "connect to consume"

upvoted 24 times

hart232 4 years, 4 months ago

Correct answer. Link below.

https://medium.com/@dan.cokely/creating-nuget-packages-in-azure-devops-with-azure-pipelines-and-yaml-d6fa30f0f15e

upvoted 3 times

NomiZm80 3 years, 12 months ago

In the link, it's not using a self-hosted agent.

upvoted 4 times

plalwa 3 years, 8 months ago

why you need to install? just connect will confirm if it can be used privately.

upvoted 2 times

xRiot007 1 year, 2 months ago

You also have to test it, not just verify that you can download it.

upvoted 2 times

chaudh Highly Voted 4 years, 3 months ago

Share package:

- Create feed
- Publish the package

Test the package:

- Connect the feed
- Install the package

upvoted 27 times

resonant 1 year, 1 month ago

You can't publish the package without connecting first to it, your answer is wrong.

upvoted 2 times

resonant 1 year, 1 month ago

"without connecting first to it" By this I mean without connecting first to the feed, of course. I can't edit my comments here in examtopics.

upvoted 1 times

hanzocodes Most Recent 8 months, 4 weeks ago

create pubs connect all

upvoted 1 times

Firdous586 10 months, 2 weeks ago

Azure Artifacts enables developers to publish and download NuGet packages from different sources such as feeds and public registries. With Azure Artifacts, you can create feeds that can be either private, allowing you to share packages with your team and specific users, or public, enabling you to share them openly with anyone on the internet.

In this article, you'll learn how to:

Create a new feed

Set up your project and connect to your feed

Publish NuGet packages
Download packages from your feed
https://learn.microsoft.com/en-us/azure/devops/artifacts/get-started-nuget?view=azure-devops&tabs=windows
upvoted 1 times

xRiot007 1 year, 2 months ago
Correct answer:
1. Create - you need a feed before doing anything
2. Connect - you need to provide in your project settings the connection details before any publish or install operation can be done
3. Publish - your feed now needs packages, so push some.
4. Install - the project can now pull and install packages from the custom feed instead of using NuGet or whatever feeds it used in the past.

References: https://learn.microsoft.com/en-us/azure/devops/artifacts/get-started-nuget?view=azure-devops&tabs=windows#create-a-feed
upvoted 5 times

zellck 1 year, 3 months ago
1. Create a new Azure Artifacts feed
2. Connect to an Azure Artifacts feed
3. Publish a package
4. Install a package

https://learn.microsoft.com/en-us/azure/devops/artifacts/get-started-nuget?view=azure-devops&tabs=windows
- How to create a new feed
- How to set up your project and connect to your feed
- How to publish NuGet packages to your feed
- How to download NuGet packages from your feed
upvoted 9 times

Maximillian 1 year, 3 months ago
From our link it says download and publish, should 3 and 4 reverse?
upvoted 1 times

resonant 1 year, 1 month ago
The link explains how to download and publish independently of one another. This doesn't mean that you have to download it first. it doesn't even make sense. How are you going to download a package from the feed if it is not published in that feed yet?
upvoted 1 times

DGladiator 1 year, 3 months ago
Create a new Azure Artifacts feed: This is where you'll be hosting your NuGet package privately. Azure Artifacts allows you to host and share packages within your organization, making it a perfect choice for your use case.

Publish a package: After creating the Azure Artifacts feed, the next step is to publish your NuGet package to this feed. You'll need to make sure you've properly configured your package for publishing, which includes providing the necessary metadata in the .nuspec file.

Connect to an Azure Artifacts feed: Once the package is published, you or your development team will need to connect to the Azure Artifacts feed to consume the package. This typically involves adding the feed to your NuGet configuration in Visual Studio or another development environment.

Install a package: The final step in verifying that the package can be consumed is to actually install it. Using the NuGet CLI or the package management functionality in your development environment, you can install the package from the Azure Artifacts feed and confirm that it works as expected.
upvoted 2 times

resonant 1 year, 1 month ago
You have to connect to the feed to consume the package, but also to publish it in the feed, so you have to connect before publishing. How are you going to publish a package to a feed without connecting first to it?
upvoted 2 times

grimstoner 1 year, 9 months ago
1. Create
2. Connect
3. Install

4. Publish

The question doesn't say anything about consuming the published package. I guess the "Install" refers to the installation of nuget and AACP as mentioned in #4 under "Connect to Feed" in this article: https://learn.microsoft.com/en-us/azure/devops/artifacts/get-started-nuget?view=azure-devops&tabs=windows#create-a-feed

upvoted 2 times

resonant 1 year, 1 month ago

Your answer is wrong. You can't isntall a package you didn't publish first. Also, what do you even mean by AACP?

upvoted 2 times

armvch 1 year, 6 months ago

The question literally says "test that package can be consumed". What do you mean doesnt say anything?

upvoted 3 times

syu31svc 2 years, 1 month ago

https://docs.microsoft.com/en-us/azure/devops/artifacts/get-started-nuget?view=azure-devops&tabs=windows#create-a-feed

1) Create a new Azure Artifacts feed
2) Publish a package
3) Connect to an Azure Artifacts feed
4) Install a package

upvoted 4 times

resonant 1 year, 1 month ago

How do you publish a package to a feed you didn't connect first? Your answer is wrong.

upvoted 1 times

Govcomm 2 years, 1 month ago

Create
Connect
Publish
Install

upvoted 5 times

UnknowMan 2 years, 4 months ago

"You need to share the package and test that the package can be consumed."
1. Create
2. Connect
2. Publish
4. Install (For test the package consuming => Already connected -> configured in Visual studio)

upvoted 3 times

jonasis 2 years, 6 months ago

1- Create a new Azure Artifacts feed
2- Connect to an Azure Artifacts feed
3- Publish a package
4- Install a package.
https://docs.microsoft.com/en-us/azure/devops/artifacts/get-started-nuget?view=azure-devops&tabs=windows#create-a-feed

upvoted 8 times

Endrit 2 years, 5 months ago

It is obvious from the link jonasis provided that this order is correct answer

upvoted 2 times

Sara_Mo 2 years, 7 months ago

the answer is correct
1. Configure
2. Create
3. Publish
4. Connect
5. Install
https://medium.com/@dan.cokely/creating-nuget-packages-in-azure-devops-with-azure-pipelines-and-yaml-d6fa30f0f15e

upvoted 1 times

photon99 2 years, 9 months ago

1. Create
2. Connect
3. Publish
4. Install

upvoted 3 times

subrata83 2 years, 11 months ago

Got this in the Az-400 exam(Sep 27 2021)

upvoted 2 times

Leo128 3 years ago

connect to the feed is difficult to place in the order as you need to connect to the feed twice - to publish and to install.

upvoted 2 times

V_Ramon 3 years, 1 month ago

this question came out today, July 28, 2021

upvoted 2 times

subrata83 3 years, 1 month ago

What was your answer

upvoted 1 times

Question #11 *Topic 5*

During a code review, you discover many quality issues. Many modules contain unused variables and empty catch blocks.
You need to recommend a solution to improve the quality of the code.
What should you recommend?

A. In a Grunt build task, select Enabled from Control Options.

B. In a Maven build task, select Run PMD.

C. In a Xcode build task, select Use xcpretty from Advanced.

D. In a Gradle build task, select Run Checkstyle.

Suggested Answer: *B*
PMD is a source code analyzer. It finds common programming flaws like unused variables, empty catch blocks, unnecessary object creation, and so forth.
There is an Apache Maven PMD Plugin which allows you to automatically run the PMD code analysis tool on your project's source code and generate a site report with its results.
Incorrect Answers:
C: xcpretty is a fast and flexible formatter for xcodebuild.
Reference:
https://pmd.github.io
/

Community vote distribution

B (100%)

AS007 Highly Voted 4 years, 4 months ago
Verified - its correct
We can use PMD and Findbugs for code analysis
upvoted 21 times

Jkmr622 Highly Voted 3 years, 8 months ago
Correctamundo dude
upvoted 8 times

FeriAZ Most Recent 6 months, 1 week ago
Selected Answer: B
PMD: (Programming Mistake Detector) is a static code analysis tool specifically designed for Java. It excels at identifying common code quality issues, including unused variables, empty catch blocks, and other potential problems.
upvoted 2 times

Sukon_Desknot 1 year, 1 month ago
Isn't PMD what finds the code issue and check for quality?
upvoted 1 times

zellck 1 year, 3 months ago
Selected Answer: B
B is the answer.

https://pmd.github.io/
PMD is a source code analyzer. It finds common programming flaws like unused variables, empty catch blocks, unnecessary object creation, and so forth.
upvoted 2 times

tjeerd 2 years, 1 month ago
Selected Answer: B
On exam 20220727.
upvoted 3 times

Govcomm 2 years, 1 month ago

Maven PMD (Problem Mistake Detection)

upvoted 1 times

Leandrocei 2 years, 2 months ago

Correct. Came today 22 july 9

upvoted 2 times

UnknowMan 2 years, 4 months ago

Selected Answer: B

correct

upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: B

correct

upvoted 1 times

Optimist_Indian 2 years, 7 months ago

Got this question in Feb-2022 exam (scored 910+). Given answer is correct. Maven PMD.

upvoted 4 times

francis6170 3 years, 2 months ago

Got this in the AZ-400 exam (June 2021).

upvoted 3 times

kumardeb 3 years, 10 months ago

B. In a Maven build task, select Run PMD.

upvoted 3 times

Rimbik 3 years, 11 months ago

B. This answer is correct.

upvoted 3 times

Question #12 *Topic 5*

Your development team is building a new web solution by using the Microsoft Visual Studio integrated development environment (IDE).
You need to make a custom package available to all the developers. The package must be managed centrally, and the latest version must be available for consumption in Visual Studio automatically.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Publish the package to a feed.

B. Create a new feed in Azure Artifacts.

C. Upload a package to a Git repository.

D. Add the package URL to the Environment settings in Visual Studio.

E. Add the package URL to the NuGet Package Manager settings in Visual Studio.

F. Create a Git repository in Azure Repos.

Suggested Answer: *ABE*
B: By using your custom NuGet package feed within your Azure DevOps (previously VSTS) instance, you'll be able to distribute your packages within your organization with ease.
Start by creating a new feed.
A: We can publish, pack and push the built project to our NuGet feed.
E: Consume your private NuGet Feed
Go back to the Packages area in Azure DevOps, select your feed and hit ɹ€Connect to feedɹ€. You'll see some instructions for your feed, but it's fairly simple to set up.
Just copy your package source URL, go to Visual Studio, open the NuGet Package Manager, go to its settings and add a new source. Choose a fancy name, insert the source URL. Done.
Search for your package in the NuGet Package Manager and it should appear there, ready for installation. Make sure to select the appropriate feed (or just all feeds) from the top right select box.
Reference:
https://medium.com/medialesson/get-started-with-private-nuget-feeds-in-azure-devops-8c7b5f022a68

Community vote distribution

ABE (100%)

Duleep Highly Voted 4 years, 1 month ago
1st: B
2nd: A
3rd: E
Answer is correct
upvoted 69 times

Jkmr622 3 years, 8 months ago
Correctamundo dude
upvoted 13 times

omw2wealth 2 years, 9 months ago
Yes dudes
upvoted 4 times

Fred64 Highly Voted 4 years, 4 months ago
Pretty sure it's correct

C: we want an automatic processs. Here we have to download the package manually
D: The menu targetted is Options/Environment. But there are many sub menus down
F: we already have a repository.
upvoted 12 times

vsvaid Most Recent 9 months ago
Selected Answer: ABE

Agree with answer
upvoted 2 times

WH16 1 year ago
Selected Answer: ABE
On exam 2023-09-06, selected A, B & E.
Score 933
upvoted 5 times

xRiot007 1 year, 2 months ago
Shouldn't the order be B, E, A ?
How are you going to push something to a feed if you don't know where the feed is located ?
upvoted 3 times

chloaus 5 months ago
Question did not ask for answers to be in correct order, just need to identify the actions required. A, B, E is fine.
upvoted 1 times

xRiot007 1 year, 1 month ago
To answer my own question, you can use the Dev console in VS to push to a nuget repository without needing to set anything up. You will need to setup a custom feed to auto pull packages during restore, so B,A,E is correct.
upvoted 2 times

Pamban 1 year, 3 months ago
Selected Answer: ABE
Correct answer: https://learn.microsoft.com/en-us/azure/devops/artifacts/get-started-nuget?view=azure-devops&tabs=windows
upvoted 2 times

zellck 1 year, 3 months ago
Selected Answer: ABE
ABE is the answer.

https://learn.microsoft.com/en-us/azure/devops/artifacts/get-started-nuget?view=azure-devops&tabs=windows
upvoted 4 times

AlexeyG 1 year, 6 months ago
got this in 02 March 2023 exams. scored 870 marks.
upvoted 3 times

nikipediaa 1 year, 7 months ago
Got this Feb 2023
upvoted 3 times

alexax578 2 years ago
Selected Answer: ABE
ABE, just the E should be "feed URL", not the "package URL"
upvoted 4 times

syu31svc 2 years, 1 month ago
Selected Answer: ABE
https://docs.microsoft.com/en-us/azure/devops/artifacts/nuget/consume?view=azure-devops&tabs=windows

Answer is ABE
upvoted 1 times

Govcomm 2 years, 1 month ago
Create
Publish
NuGet PM setting in Visual Studio
upvoted 1 times

Leandrocei 2 years, 2 months ago
Correct. Came today 22 july 9
upvoted 1 times

UnknowMan 2 years, 4 months ago

correct

upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: ABE

correct

upvoted 2 times

goatlord 3 years, 1 month ago

Bigly Correct

upvoted 1 times

kumardeb 3 years, 10 months ago

A. Publish the package to a feed.

B. Create a new feed in Azure Artifacts.

E. Add the package URL to the NuGet Package Manager settings in Visual Studio.

upvoted 3 times

Question #13 *Topic 5*

You use GitHub for source control.
A file that contains sensitive data is committed accidentally to the Git repository of a project.
You need to delete the file and its history form the repository.
Which two tools can you use? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. the git filter-branch command

B. BFG Repo-Cleaner

C. the git rebase command

D. GitHub Desktop

Suggested Answer: *AB*
To entirely remove unwanted files from a repository's history you can use either the git filter-branch command or the BFG Repo-Cleaner open source tool.
Reference:
https://docs.github.com/en/github/authenticating-to-github/keeping-your-account-and-data-secure/removing-sensitive-data-from-a-repository

Community vote distribution
AB (100%)

knvenkat123 Highly Voted 2 years, 1 month ago
Selected Answer: AB
BFG Repo cleaner is an alternative to git filter-branch. It can be used to remove sensitive data or large files that were committed wrongly like binaries compiled from the source. It is written in Scala. Project website: BFG Repo Cleaner
upvoted 8 times

surensaluka Highly Voted 1 year, 7 months ago
Selected Answer: AB
This question came today (2023-02-14). Answers came as pair of 2 commands.
upvoted 6 times

vsvaid Most Recent 9 months ago
Selected Answer: AB
Agree with given answer
upvoted 2 times

zellck 1 year, 3 months ago
Selected Answer: AB
AB is the answer.

https://docs.github.com/en/authentication/keeping-your-account-and-data-secure/removing-sensitive-data-from-a-repository#using-the-bfg
The BFG Repo-Cleaner is a tool that's built and maintained by the open source community. It provides a faster, simpler alternative to git filter-repo for removing unwanted data.
upvoted 5 times

zellck 1 year, 3 months ago
https://git-scm.com/docs/git-filter-branch#_description
Lets you rewrite Git revision history by rewriting the branches mentioned in the <rev-list options>, applying custom filters on each revision. Those filters can modify each tree (e.g. removing a file or running a perl rewrite on all files) or information about each commit. Otherwise, all information (including original commit times or merge information) will be preserved.
upvoted 3 times

Power123 1 year, 8 months ago
BFG Repo cleaner is an alternative to git filter-branclt is h. It can be used to remove sensitive data or large files that were committed wrongly like binaries compiled from the source. Project website: BFG Repo Cleaner
upvoted 2 times

alexax578 2 years ago

Selected Answer: AB

It is git-filter-repo now (+ BFG Repo-Cleaner)

"To entirely remove unwanted files from a repository's history you can use either the git filter-repo tool or the BFG Repo-Cleaner open source tool."

https://docs.github.com/en/authentication/keeping-your-account-and-data-secure/removing-sensitive-data-from-a-repository

upvoted 4 times

syu31svc 2 years, 1 month ago

Selected Answer: AB

Given link supports A and B as the answers

upvoted 2 times

az_architect 2 years, 1 month ago

Thanks Jay158. The provided link explain very well that
git filter-branch and BFG are the correct options.

upvoted 2 times

Govcomm 2 years, 1 month ago

git filter-branch
BFG

upvoted 2 times

Eltooth 2 years, 3 months ago

Selected Answer: AB

A and B are correct answers.

upvoted 3 times

jay158 2 years, 4 months ago

Answer is correct
https://docs.github.com/en/authentication/keeping-your-account-and-data-secure/removing-sensitive-data-from-a-repository

upvoted 3 times

Question #14 *Topic 5*

Your company uses GitHub for source control. The company has a team that performs code reviews.
You need to automate the assignment of the code reviews. The solution must meet the following requirements:
➪ Prioritize the assignment of code reviews to team members who have the fewest outstanding assignments.
➪ Ensure that each team member performs an equal number of code reviews in any 30-day period.
➪ Prevent the assignment of code reviews to the team leader.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Clear Never assign certain team members.

B. Select If assigning team members, don't notify the entire team.

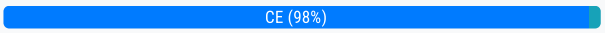
C. Select Never assign certain team members.

D. Set Routing algorithm to Round robin.

E. Set Routing algorithm to Load balance.

Suggested Answer: *AE*
A: To always skip certain members of the team, select Never assign certain team members. Then, select one or more team members you'd like to always skip. In this case select the team leader.
E: The load balance algorithm chooses reviewers based on each member's total number of recent review requests and considers the number of outstanding reviews for each member. The load balance algorithm tries to ensure that each team member reviews an equal number of pull requests in any 30 day period.
Incorrect Answers:
D: The round robin algorithm chooses reviewers based on who's received the least recent review request, focusing on alternating between all members of the team regardless of the number of outstanding reviews they currently have.
Reference:
https://docs.github.com/en/organizations/organizing-members-into-teams/managing-code-review-assignment-for-your-team

Community vote distribution



syu31svc Highly Voted 2 years, 1 month ago
Selected Answer: CE
https://docs.github.com/en/organizations/organizing-members-into-teams/managing-code-review-settings-for-your-team

"Optionally, to always skip certain members of the team, select Never assign certain team members. Then, select one or more team members you'd like to always skip" ---> C (prevent assignment to Leader)

"The load balance algorithm chooses reviewers based on each member's total number of recent review requests and considers the number of outstanding reviews for each member. The load balance algorithm tries to ensure that each team member reviews an equal number of pull requests in any 30 day period." ---> E (Ensure that each team member performs an equal number of code reviews in any 30-day period)
upvoted 18 times

AnishGS Most Recent 6 months ago
Selected Answer: CE
Tested in lab account
upvoted 1 times

vsvaid 9 months ago
Selected Answer: CE
C and E
upvoted 1 times

fafda 1 year, 2 months ago
Selected Answer: CE
CE. Select Never assign certain team members is option C not A.
upvoted 2 times

zellck 1 year, 3 months ago

Selected Answer: CE

CE is the answer.

https://docs.github.com/en/organizations/organizing-members-into-teams/managing-code-review-settings-for-your-team#routing-algorithms
The load balance algorithm chooses reviewers based on each member's total number of recent review requests and considers the number of outstanding reviews for each member. The load balance algorithm tries to ensure that each team member reviews an equal number of pull requests in any 30 day period.

upvoted 4 times

zellck 1 year, 3 months ago

https://docs.github.com/en/organizations/organizing-members-into-teams/managing-code-review-settings-for-your-team#configuring-auto-assignment
Optionally, to always skip certain members of the team, select Never assign certain team members. Then, select one or more team members you'd like to always skip.

upvoted 2 times

az_architect 2 years, 1 month ago

CE options are logically correct. However, I have not tried the options practically.

upvoted 3 times

Govcomm 2 years, 1 month ago

Never assign specific team member. i.e. The team leader
Load balancing

upvoted 1 times

Leandrocei 2 years, 2 months ago

Selected Answer: CE

CE. Came today 22 july 9

upvoted 4 times

Redimido 2 years, 2 months ago

Selected Answer: CE

1. The load balance algorithm chooses reviewers based on each member's total number of recent review requests and considers the number of outstanding reviews for each member. The load balance algorithm tries to ensure that each team member reviews an equal number of pull requests in any 30 day period.
2. Optionally, to always skip certain members of the team, select Never assign certain team members. Then, select one or more team members you'd like to always skip.

upvoted 3 times

Eltooth 2 years, 4 months ago

Selected Answer: CE

Correct answer - C & E.

upvoted 3 times

zuzu_toggler 2 years, 4 months ago

Selected Answer: CE

CE is correct.

upvoted 2 times

UnknowMan 2 years, 4 months ago

Selected Answer: CE

CE is correct

upvoted 2 times

UnknowMan 2 years, 4 months ago

CE is correct

upvoted 2 times

jay158 2 years, 4 months ago

Selected Answer: CE

https://docs.github.com/en/organizations/organizing-members-into-teams/managing-code-review-settings-for-your-team

upvoted 4 times

Brexten 2 years, 4 months ago

Provided answer and choice do not match, perhaps some mix up. Should be C&E

upvoted 2 times

Pandur1 2 years, 4 months ago

So I guess that should be C&E (instead of A&E)

upvoted 1 times

U3 2 years, 4 months ago

I think C&E

upvoted 2 times

Question #15 *Topic 5*

You have a GitHub repository.
You create a new repository in Azure DevOps.
You need to recommend a procedure to clone the repository from GitHub to Azure DevOps.
What should you recommend?

A. Create a pull request.

B. Create a webhook.

C. Create a service connection for GitHub.

D. From Import a Git repository, click Import.

E. Create a personal access token in Azure DevOps.

Suggested Answer: *D*
You can import an existing Git repo from GitHub, Bitbucket, GitLab, or other location into a new or empty existing repo in your project in Azure DevOps.

Import into a new repo -
➪ Select Repos, Files.
➪ From the repo drop-down, select Import repository.
➪ If the source repo is publicly available, just enter the clone URL of the source repository and a name for your new Git repository.
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/git/import-git-repository?view=azure-devops

Community vote distribution
D (100%)

AS007 Highly Voted 4 years, 4 months ago
Correct Answer - Verified
upvoted 38 times

Fred64 Highly Voted 4 years, 4 months ago
Import Repository inside Repos/Files after creating the project
upvoted 5 times

zellck Most Recent 1 year, 3 months ago
Selected Answer: D
D is the answer.

https://learn.microsoft.com/en-us/azure/devops/repos/git/import-git-repository?view=azure-devops#import-into-a-new-repo
upvoted 3 times

az_architect 2 years, 1 month ago
The import Git repo is the correct answer.
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: D
If you've done your own hands-on, D is the answer
upvoted 2 times

Govcomm 2 years, 1 month ago
Import a Git repository
upvoted 1 times

kennynelcon 2 years, 2 months ago
Selected Answer: D
Correct answer and explanation.
Lab Tested

upvoted 1 times

Eltooth 2 years, 3 months ago

Selected Answer: D

D is correct answer.

upvoted 1 times

UnknowMan 2 years, 4 months ago

correct

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: D

correct answer and explanation

upvoted 1 times

sidharthwader 2 years, 8 months ago

Correct answer verified!

upvoted 1 times

aroravibhu 2 years, 9 months ago

Selected Answer: D

D it is

upvoted 1 times

rajvelm 2 years, 10 months ago

Got this questions on 7 Nov 2021

upvoted 1 times

Ashutosh_9608 2 years, 11 months ago

https://docs.microsoft.com/en-us/azure/devops/repos/git/import-git-repository?view=azure-devops

upvoted 1 times

Kalaismile06 3 years, 3 months ago

From Import Git repository is the right answer

upvoted 1 times

Miles19 3 years, 5 months ago

correct

upvoted 1 times

RKS 3 years, 7 months ago

Verified - Correct!

upvoted 2 times

Question #16 *Topic 5*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
The lead developer at your company reports that adding new application features takes longer than expected due to a large accumulated technical debt.
You need to recommend changes to reduce the accumulated technical debt.
Solution: You recommend increasing the code duplication.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Instead reduce the code complexity.
Note: Technical debt is the accumulation of sub-optimal technical decisions made over the lifetime of an application. Eventually, it gets harder and harder to change things: it's the 'sand in the gears' that sees IT initiatives grind to a halt.
Reference:
https://dzone.com/articles/fight-through-the-pain-how-to-deal-with-technical https://www.devopsgroup.com/blog/five-ways-devops-helps-with-technical-debt/

Community vote distribution
B (100%)

jasifu3 Highly Voted 2 years, 6 months ago
Selected Answer: B
probably the easiest question in the exam. Imagine telling the lead dev that MORE duplication is how you reduce technical debt lol
upvoted 20 times

Mattt 3 months, 3 weeks ago
That means code complexity
upvoted 1 times

WH16 Most Recent 1 year ago
Selected Answer: B
On exam 2023-09-06, selected B.
upvoted 2 times

Tyler2023 1 year ago
definitely no, you need to submit your resignation letter when you recommend this.
upvoted 1 times

zellck 1 year, 3 months ago
Selected Answer: B
B is the answer.

https://learn.microsoft.com/en-us/training/modules/identify-technical-debt/2-examine-code-quality
Reusability measures whether existing assets—such as code—can be used again. Assets are more easily reused if they have modularity or loose coupling characteristics. The number of interdependencies can measure reusability. Running a static analyzer can help you identify these interdependencies.
upvoted 1 times

ubuntu1234 2 years ago
On the opposite side ,Does "Decreasing" code duplication , reduces technical debt?
upvoted 2 times

syu31svc 2 years, 1 month ago

Selected Answer: B

Instead reduce the code complexity.

Answer is No

upvoted 2 times

az_architect 2 years, 1 month ago

Code duplication would rather increase the existing technical debt.

Hence answer is: B

upvoted 1 times

franekfranek 2 years, 3 months ago

Selected Answer: B

Please Microsoft add more questions like that so I can pass the exam lol

upvoted 4 times

currotron 2 years, 2 months ago

Jajaja

upvoted 1 times

Eltooth 2 years, 3 months ago

Selected Answer: B

B is correct answer.

upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 1 times

rdemontis 2 years, 6 months ago

Selected Answer: B

correct and obvious

upvoted 1 times

V_Ramon 3 years, 1 month ago

this question came out today, July 28, 2021

upvoted 3 times

ukohae39 3 years, 2 months ago

Correct

upvoted 2 times

Miles19 3 years, 5 months ago

Correct.

upvoted 4 times

Question #17 *Topic 5*

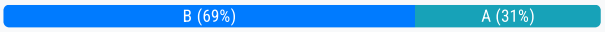
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
The lead developer at your company reports that adding new application features takes longer than expected due to a large accumulated technical debt.
You need to recommend changes to reduce the accumulated technical debt.
Solution: You recommend increasing the test coverage.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Instead reduce the code complexity.
Note: Technical debt is the accumulation of sub-optimal technical decisions made over the lifetime of an application. Eventually, it gets harder and harder to change things: it's the 'sand in the gears' that sees IT initiatives grind to a halt.
Reference:
https://dzone.com/articles/fight-through-the-pain-how-to-deal-with-technical https://www.devopsgroup.com/blog/five-ways-devops-helps-with-technical-debt/

Community vote distribution



Beast_Hollow Highly Voted 3 years, 4 months ago
B is correct, cause just adding test coverages won't reduce the technical debt.
upvoted 36 times

samyderlachs 2 years, 7 months ago
Dave Farley would say sth. else here. Usaly it reduces technical debt cause you start to refactor things. You wouldnt just write tests for bad code.
upvoted 3 times

pj74 2 years, 1 month ago
But the point of tests is they enable you to refactor the code with more confidence... the existing tests don't change as you reduce technical debt, it's the underlying code being tested that is improved. Agree that changing test coverage can be a supporting factor in reducing technical debt, but by itself doesn't reduce technical debt.
upvoted 2 times

zeaimen 1 year, 2 months ago
Typical non sense binary question (tests required to refactor with confidence)
upvoted 1 times

mfawew223 9 months, 3 weeks ago
We are recommending changes to reduce technical debt. Increasing test coverage doesnt have to solve the problem itself to be a "good" recommendation.

I think test coverage is effective if there is large, unmanaged technical debt. It can identify areas that could be improved, complexity reduced, or otherwise streamlined. But that effect will have a diminishing return as the backlog of technical debt is resolved. When the returns have diminished past a certain point, the test coverage can probably be scaled back.

Since the scenario presented states that there is a large accumulated technical debt, I believe the answer is Yes for this case.
upvoted 1 times

Mithi Highly Voted 3 years, 10 months ago

Yes, this can also help. If the test coverage is high , that means you know parts of the code that are not being used at all. This can help you refactor code snippets to see if they are required or not.
upvoted 19 times

ArnoudBM 3 years, 9 months ago
And unit testing is an almost required ingredient for checking your refactoring results
upvoted 4 times

Miles19 3 years, 4 months ago
Yes, I believe you're right. By increasing the code coverage on the unit tests, we are making sure that classes and methods are doing what they are supposed to do - meaning this is definitely contributing decreasing the technical debt.
upvoted 4 times

arr73 Most Recent 4 months, 2 weeks ago
Selected Answer: A
A is correct. The link below is the reference in Microsoft Learn documentation. It says "One key way to minimize the constant acquisition of technical debt is to use automated testing and assessment." --> more automated testing --> higher test coverage
https://learn.microsoft.com/en-us/training/modules/identify-technical-debt/4-introduction-technical-debt
upvoted 3 times

vsvaid 9 months ago
Selected Answer: A
I think yes
upvoted 1 times

Tyler2023 1 year ago
I don't think adding test coverage will help reduce the technical debt. Unit tests and integration tests are only specifications that will make sure no one break the logic of the code
upvoted 1 times

Tyler2023 1 year ago
My answer is 50/50 :D, I don't know, it depends after reading other comments, all their reasoning are valid
upvoted 1 times

yana_b 1 year, 1 month ago
https://learn.microsoft.com/en-us/azure/devops/pipelines/test/review-code-coverage-results?view=azure-devops

Reviewing the code coverage result helps to identify code path(s) that are not covered by the tests. This information is important to improve the test collateral over time by reducing the test debt.
upvoted 1 times

renzoku 1 year, 3 months ago
you can get 100% test coverage but your technical debt won't be solved
upvoted 3 times

Fal991l 1 year, 5 months ago
GPT: Yes, increasing test coverage can help reduce accumulated technical debt [^A^]. By writing more tests to cover more of the codebase, you can improve the quality of the code and make it easier to identify and fix issues. This can help prevent the accumulation of technical debt and make it easier to add new features to the application.

So, the correct answer to your question is A. Yes.
upvoted 1 times

catfood 1 year, 2 months ago
you know GPT can be confidently wrong on basic things, I'm not liking all these comments where someone has just pasted AI responses.....
upvoted 6 times

Hieronimusov 1 year, 7 months ago
Selected Answer: B
test coverages dont check your coding style, spelling and code duplication. It just checks functionality it check if :

var 123urass = true ? 1 : 0;
var 123uranus = false ? 0 : 1
Assert 123urass == 123uranus == true

oooh cool it passes.
upvoted 6 times

xRiot007 1 year, 2 months ago
Technical debt is not just coding style, but overall design, the performance and functionality of that design and how many issues (code smells, bugs, etc) are in your codebase.
upvoted 1 times

SayCloud 1 year, 7 months ago
Selected Answer: A
I think it should be A,
Regular and timely testing, process automation, or increased testing coverage help reduce technical debt.
https://ardas-it.com/how-to-reduce-technical-debt-best-strategies-for-technical-debt-reduction
upvoted 1 times

DavidCarp 1 year, 9 months ago
Selected Answer: B
Would consider B as the answer. Not seeing the relationship with test coverage.
The more test coverage, means that more of your code is under some control, but that doesn't mean that you are still introducing issues that will be part of technical debt, i.e, code does what is supposed to do, but might fail sooner or later, either do to the deprecation of what is being used,...
upvoted 3 times

GokhanSenyuz 1 year, 10 months ago
Selected Answer: B
answer clear No
upvoted 3 times

ehurfheiz 1 year, 11 months ago
Selected Answer: B
I think it doesn't reduce the technical debt
upvoted 3 times

giuliohome 2 years ago
Selected Answer: A
https://www.opkey.com/blog/technical-debt-what-does-it-mean-to-be-in-the-red-with-qa-testing
The key contributors in accumulating technical debt in a QA practice include: a lack of test coverage, oversized user stories, short sprints, and cutting corners due to delivery pressures.
upvoted 2 times

WickedMJ 2 years ago
Selected Answer: B
B is correct since reducing code complexity should be the right answer to these technical debt problem
upvoted 3 times

tempura108 2 years ago
Selected Answer: B
Increasing test coverage ensures your UnitTest runs through that block of code.
upvoted 3 times

syu31svc 2 years, 1 month ago
Selected Answer: A
https://docs.microsoft.com/en-us/azure/devops/pipelines/test/review-code-coverage-results?view=azure-devops

"Code coverage helps you determine the proportion of your project's code that is actually being tested by tests such as unit tests. To increase your confidence of the code changes, and guard effectively against bugs, your tests should exercise - or cover - a large proportion of your code.

Reviewing the code coverage result helps to identify code path(s) that are not covered by the tests. This information is important to improve the test collateral over time by reducing the test debt."

I would say Yes
upvoted 2 times

Question #18 *Topic 5*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
The lead developer at your company reports that adding new application features takes longer than expected due to a large accumulated technical debt.
You need to recommend changes to reduce the accumulated technical debt.
Solution: You recommend reducing the code complexity.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
Note: Technical debt is the accumulation of sub-optimal technical decisions made over the lifetime of an application. Eventually, it gets harder and harder to change things: it's the 'sand in the gears' that sees IT initiatives grind to a halt.
Reference:
https://dzone.com/articles/fight-through-the-pain-how-to-deal-with-technical https://www.devopsgroup.com/blog/five-ways-devops-helps-with-technical-debt/

Community vote distribution

A (100%)

crutester Highly Voted 3 years, 9 months ago
Answer is correct!
upvoted 12 times

Kalaismile06 Highly Voted 3 years, 3 months ago
Decreasing code complexity always save the developer times.
upvoted 5 times

WH16 Most Recent 1 year ago
Selected Answer: A
On exam 2023-09-06, selected A.
upvoted 3 times

syu31svc 2 years, 1 month ago
Selected Answer: A
This is correct
upvoted 1 times

az_architect 2 years, 1 month ago
Agree with the provided answer and the explanation
upvoted 1 times

Eltooth 2 years, 3 months ago
Selected Answer: A
A is correct answer.
upvoted 1 times

UnknowMan 2 years, 4 months ago
Selected Answer: A
Correct
upvoted 1 times

rdemontis 2 years, 6 months ago
Selected Answer: A
correct of course

upvoted 1 times

awron_durat 2 years, 7 months ago

Selected Answer: A

Reducing code complexity will decrease the difficulty of developing new code and lead to a decreased tech debt.

upvoted 2 times

V_Ramon 3 years, 1 month ago

this question came out today, July 28, 2021

upvoted 2 times

mg37 3 years, 3 months ago

correct

upvoted 3 times

Dekai 3 years, 3 months ago

Correct

upvoted 3 times

Miles19 3 years, 5 months ago

Correct.

upvoted 4 times

Question #19 *Topic 5*

During a code review, you discover quality issues in a Java application.
You need to recommend a solution to detect quality issues including unused variables and empty catch blocks.
What should you recommend?

A. In a Maven build task, select Run PMD.

B. In an Xcode build task, select Use xcpretty from Advanced.

C. In a Gulp build task, specify a custom condition expression.

D. In a Grunt build task, select Enabled from Control Options.

Suggested Answer: *A*
PMD is a source code analyzer. It finds common programming flaws like unused variables, empty catch blocks, unnecessary object creation, and so forth.
There is an Apache Maven PMD Plugin which allows you to automatically run the PMD code analysis tool on your project's source code and generate a site report with its results.
Incorrect Answers:
B: xcpretty is a fast and flexible formatter for xcodebuild.
Reference:
https://pmd.github.io/

Community vote distribution
A (100%)

kumardeb Highly Voted 3 years, 10 months ago
A. In a Maven build task, select Run PMD.
upvoted 12 times

chingdm 1 year, 8 months ago
PMD stands for Programming Mistake Detector https://www.sfdcstop.com/2017/12/analyze-your-apex-code-using-pmd-source.html
upvoted 1 times

UrbanRellik Most Recent 3 months, 3 weeks ago
Selected Answer: A
A. Maven build task > Run PMD.
upvoted 1 times

vsvaid 9 months ago
Selected Answer: A
Agree with A
upvoted 1 times

zellck 1 year, 3 months ago
Same as Question 11.
https://www.examtopics.com/discussions/microsoft/view/20515-exam-az-400-topic-5-question-11-discussion
upvoted 4 times

zellck 1 year, 3 months ago
Selected Answer: A
A is the answer.

https://pmd.github.io/
PMD is a source code analyzer. It finds common programming flaws like unused variables, empty catch blocks, unnecessary object creation, and so forth.
upvoted 2 times

tjeerd 2 years, 1 month ago
Selected Answer: A
On exam 20220727.

upvoted 3 times

az_architect 2 years, 1 month ago

Maven PDM plugin, Hence given answer choice is correct.

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: A

"Java application"

A is the answer; Maven

upvoted 1 times

Govcomm 2 years, 1 month ago

Run PMD

upvoted 1 times

Leandrocei 2 years, 2 months ago

Correct. Came today 22 july 9

upvoted 2 times

Eltooth 2 years, 3 months ago

Selected Answer: A

A is correct answer.

upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 2 times

rdemontis 2 years, 6 months ago

Selected Answer: A

answer and explanations are correct

upvoted 2 times

Optimist_Indian 2 years, 7 months ago

Got this question in Feb-2022 exam (scored 910+). Given answer is correct. A - PMD.

upvoted 2 times

subrata83 2 years, 11 months ago

Got this in the Az-400 exam(Sep 27 2021)

upvoted 3 times

francis6170 3 years, 2 months ago

Got this in the AZ-400 exam (June 2021).

upvoted 3 times

ArnoudBM 3 years, 9 months ago

Topic 1, question 8

upvoted 4 times

Question #20 *Topic 5*

You use Azure Artifacts to host NuGet packages that you create.
You need to make one of the packages available to anonymous users outside your organization. The solution must minimize the number of publication points.
What should you do?

A. Change the feed URL of the package

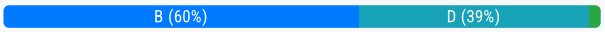
B. Create a new feed for the package

C. Promote the package to a release view.

D. Publish the package to a public NuGet repository.

Suggested Answer: *B*
Azure Artifacts introduces the concept of multiple feeds that you can use to organize and control access to your packages.
Packages you host in Azure Artifacts are stored in a feed. Setting permissions on the feed allows you to share your packages with as many or as few people as your scenario requires.
Feeds have four levels of access: Owners, Contributors, Collaborators, and Readers.
Reference:
https://docs.microsoft.com/en-us/azure/devops/artifacts/feeds/feed-permissions?view=vsts&tabs=new-nav

Community vote distribution



TosO Highly Voted 4 years, 5 months ago
The only possible correct answer is: Publish the package to a public NuGet repository.
This is because to use the public feed feature in Azure DevOps, the project itself must be public:
"Public feeds are project-scoped feeds that live inside a public project. You cannot convert an existing organization-scoped feed into a project-scoped feed or a public feed." https://docs.microsoft.com/en-us/azure/devops/artifacts/tutorials/share-packages-publicly?view=azure-devops
upvoted 63 times

Marang73 3 years, 10 months ago
Nothing is mentioned in the question that the project is private.
upvoted 8 times

prashantjoge 2 years, 5 months ago
You need to make one of the packages available to anonymous users outside your organization.
upvoted 2 times

rdemontis 2 years, 6 months ago
totally agree with you
upvoted 1 times

rdemontis 2 years, 5 months ago
On second thought perhaps the answer provided is correct. In fact, we don't have anything to be sure that the project is private. It could easily be public and use a Feed with scope = organization. In such a case it would be enough to create a new public feed to solve the problem and satisfy the requirement "The solution must minimize the number of publication points".
upvoted 2 times

prashantjoge 2 years, 5 months ago
This is correct. If a project is private the its feed is private. If a project is public, the feed also becomes public. Questions says only one package needs to be made public
upvoted 2 times

sanhoo 3 years, 1 month ago
Examtopic's answer is correct. refer the link shared by droy89's
upvoted 3 times

webforce08 Highly Voted 4 years, 9 months ago
Correct
upvoted 20 times

Skankhunt Most Recent 1 month, 3 weeks ago

The package is already in Azure Artifacts, one of the requirements is "The solution must minimize the number of publication points" - thus option B is correct.

upvoted 1 times

sondrex 2 months ago

The correct answer is D: Publish the package to a public NuGet repository.

Here's why:

NuGet Package Repository (Public):
Hosting the package in a public NuGet repository makes it accessible to anyone, including anonymous users outside your organization.
No authentication is required, which meets the goal of external accessibility.
Minimizing Publication Points:
By using a public NuGet repository, you maintain just one publication point. No need for additional feeds or complex setups.
Other Options Explained:
New Feed for the Package: While creating a new feed is an option, it introduces unnecessary complexity and additional publication points.
Release View in Azure Artifacts: Release views are useful for managing package visibility within different environments, but they don't address the requirement for external accessibility.

upvoted 1 times

FeriAZ 5 months, 3 weeks ago

Selected Answer: D

Minimized Publication Points: Leveraging an existing public repository eliminates the need for additional infrastructure or configuration within Azure Artifacts, keeping the number of publication points to a minimum.
Public Accessibility: Public repositories like nuget.org are readily accessible by anonymous users searching for NuGet packages.

upvoted 2 times

ozbonny 6 months, 3 weeks ago

Selected Answer: D

Correct D

upvoted 1 times

hardinxcore 8 months, 3 weeks ago

Selected Answer: D

Note that publishing to a public repository, e.g. nuget.org doesn't necessarily increase the number of publication points, because nuget.org is the main goto for public dependencies. Therefore it is likely that's already being used. In contrast, creating a new feed will at least add one extra publication point.

upvoted 2 times

vsvaid 9 months ago

Selected Answer: D

D for me

upvoted 1 times

Firdous586 10 months, 2 weeks ago

https://devblogs.microsoft.com/devops/share-packages-publicly-from-azure-artifacts-public-preview/#:~:text=NuGet%2C%20npm%2C%20Maven%2C%20and,the%20top%20of%20the%20UI.

upvoted 1 times

Sukon_Desknot 1 year ago

Selected Answer: B

The answer is B.

D is not the answer because
to Publish the package to a public NuGet repository: While this would make the package publicly accessible, it doesn't involve Azure Artifacts. Plus, the goal is to minimize publication points, and using external public repositories may add complexity.

upvoted 2 times

yana_b 1 year, 1 month ago

Selected Answer: B

Answer is B

To share your packages publicly, you can simply share your feed URL e.g. https://dev.azure.com/<ORGANIZATION_NAME>/<PROJECT-NAME>/_artifacts/feed/<FEED_NAME> or share individual packages with package badges.

As long as your project is kept public, anyone can view and download packages from your public feed. Anonymous users won't be able to create new feeds or access the recycle bin.

Reference: https://learn.microsoft.com/en-us/azure/devops/artifacts/tutorials/share-packages-publicly?view=azure-devops&tabs=nuget
upvoted 1 times

Sukon_Desknot 1 year, 1 month ago

Selected Answer: D

For those picking B, I wonder why because it literally doesn't mention anything about the feed being public or not
upvoted 2 times

renzoku 1 year, 1 month ago

Selected Answer: D

It should be "D"
NuGet package repository
Public repository hosted externally
No authentication required to anyone(available to anonymous users outside your organization)
One publication point (minimize the number of publication points)

New Feed for the Package
Private view within Azure Artifacts, Authentication required to external users, Organizing packages for different projects or teams.

Release View in Azure Artifacts
Private view within Azure Artifacts, Authentication required to external users, Managing package visibility through various environments/stages.
upvoted 2 times

resonant 1 year, 1 month ago

Why isn't C the correct answer?
upvoted 1 times

resonant 1 year ago

Because promoting to a release view doesn't mean it will be public to anonymous users
upvoted 1 times

Aravindking 1 year, 3 months ago

Selected Answer: B

Creating a new feed for the package would also make it available to anonymous users outside your organization, but it would require you to create a new publication point. This would add an additional layer of complexity to managing and maintaining your packages, as you would need to keep track of two separate feeds.

If you only need to make one package available to anonymous users, then creating a new feed is a viable option. However, if you need to make multiple packages available to anonymous users, then it is more efficient to publish them to a public NuGet repository.
upvoted 2 times

zeaimen 1 year, 2 months ago

if it's more complex to create new feed than publishing package, then why you choose it ? (why b instead of d ?)
upvoted 1 times

zellck 1 year, 3 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/devops/artifacts/tutorials/share-packages-publicly?view=azure-devops&tabs=nuget
Azure Artifacts provides an easy way to share packages to users outside your organization and even external customers using public feeds. Packages that are stored in public feeds can be restored and installed by anyone on the Internet.
upvoted 3 times

DGladiator 1 year, 3 months ago

GPT4
D. Publish the package to a public NuGet repository.

Azure Artifacts doesn't currently support anonymous access (as of my knowledge cut-off in September 2021). As such, the best way to make a NuGet package available to anonymous users would be to publish the package to a public repository, such as nuget.org, where anyone can access it.

The other options (A, B, and C) all involve manipulation within Azure Artifacts, which still would not allow for anonymous access. Changing the feed URL or creating a new feed doesn't allow anonymous access, and promoting the package to a release view also doesn't grant anonymous access.

Remember to always double check the Azure documentation or the Azure portal itself for updates, as Azure is a rapidly evolving service and changes may have occurred since my training data was last updated in September 2021.

upvoted 2 times

Question #21 *Topic 5*

You use GitHub for source control and project-related discussions.
You receive a notification when an entry is made to any team discussion.
You need to ensure that you receive email notifications only for discussions in which you commented or in which you are mentioned.
Which two Notifications settings should you clear? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Automatically watch teams

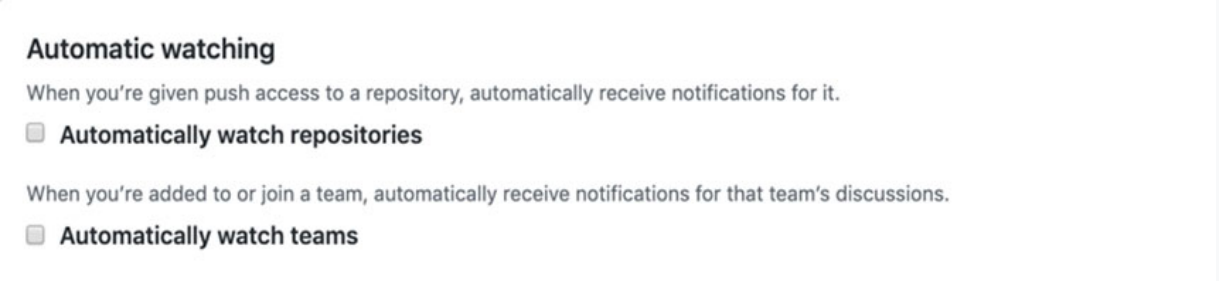
B. Participating

C. Automatically watch repositories

D. Watching

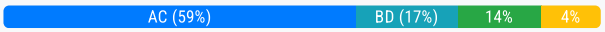
Suggested Answer: *BC*
C: If "Automatically watch repositories" is disabled, then you will not automatically watch your own repositories. You must navigate to your repository page and choose the watch option.

A, C: Automatic watching -
By default, anytime you gain access to a new repository, you will automatically begin watching that repository. Anytime you join a new team, you will automatically be subscribed to updates and receive notifications when that team is @mentioned. If you don't want to automatically be subscribed, you can unselect the automatic watching options.



Incorrect:
Not D: When you watch a repository, you're subscribing to updates for activity in that repository. Similarly, when you watch a specific team's discussions, you're subscribing to all conversation updates on that team's page.
Reference:
https://docs.github.com/en/account-and-profile/managing-subscriptions-and-notifications-on-github/setting-up-notifications/configuring-notifications

Community vote distribution



Divyayuvi Highly Voted 2 years ago
Selected Answer: AC
IMO A&C is the answer
upvoted 15 times

syu31svc Highly Voted 2 years ago
Selected Answer: BD
From provided link

"If you don't want notifications to be sent to your email, unselect email for participating and watching notifications.
If you want to receive notifications by email when you've participated in a conversation, then you can select email under "Participating".
If you do not enable watching or participating notifications for web and mobile, then your notifications inbox will not have any updates."

I would take B and D
upvoted 13 times

NK203 1 year, 5 months ago
Which two Notifications settings should you clear?clear!clear!

upvoted 7 times

vsvaid Most Recent 9 months ago

Selected Answer: AC

A and C for me

upvoted 4 times

itguy2 10 months, 3 weeks ago

A and D are correct.A.

Automatically watch teams - clear this - Anytime you join a new team, you will automatically be subscribed to updates and receive notification when that team is @mentioned.

B. Participating - don't clear this - Notifications for the conversations you are participating in, or if someone cites you with an @mention.

C. Automatically watch repositories - doesn't matter - Notifications for all repositories, teams, or conversations you're watching.

D. Watching - clear this -Notifications for all repositories, teams, or conversations you're watching.

upvoted 2 times

gabo 11 months, 3 weeks ago

Anytime you join a new team, you will automatically be subscribed to updates and receive notifications when that team is @mentioned, so A cannot be the answer.

upvoted 1 times

ghabool 1 year ago

I choose B, D

In Github, Under Default notification settings, choose how you want to receive notifications for each of the following categories:

Participating: These notifications are sent when you participate in a conversation or someone brings you into one by @mentioning your username1. You can choose to receive these notifications by email, web, or both.

Watching: These notifications are sent when you’re watching a repository1. You can choose to receive these notifications by email, web, or both, or disable them entirely.

Your activity: These notifications are sent when there is activity on issues and pull requests you’ve created1. You can choose to receive these notifications by email, web, or both, or disable them entirely.

upvoted 2 times

yana_b 1 year, 1 month ago

Selected Answer: AC

It is all mentioned in the link below

https://docs.github.com/en/account-and-profile/managing-subscriptions-and-notifications-on-github/setting-up-notifications/configuring-notifications#automatic-watching

upvoted 3 times

Aravindking 1 year, 3 months ago

Selected Answer: AD

The correct answers are A and D.

The "Automatically watch teams" setting will cause you to receive notifications for all discussions in any team that you are a member of. The "Watching" setting will cause you to receive notifications for all discussions in any repository that you are watching.

To ensure that you receive email notifications only for discussions in which you commented or in which you are mentioned, you should clear both of these settings. This will ensure that you only receive notifications for discussions that you are directly involved in.

upvoted 3 times

zellck 1 year, 3 months ago

Selected Answer: AC

AC is the answer.

https://docs.github.com/en/account-and-profile/managing-subscriptions-and-notifications-on-github/setting-up-notifications/configuring-notifications#automatic-watching

By default, anytime you gain access to a new repository, you will automatically begin watching that repository. Anytime you join a new team, you

will automatically be subscribed to updates and receive notifications when that team is @mentioned. If you don't want to automatically be subscribed, you can unselect the automatic watching options in your notification settings.
upvoted 8 times

DGladiator 1 year, 3 months ago
GPT4
The two notification settings that you should clear to achieve the desired result are:

A. Automatically watch teams
This setting automatically subscribes you to all team discussions, so you receive notifications for all entries. Disabling this ensures you don't get notified unless you're participating in a discussion or mentioned.

C. Automatically watch repositories
When you're automatically watching a repository, you get notified of all activity. Clearing this option would stop these notifications and ensure you only receive notifications for discussions you're participating in or mentioned.

Option B, Participating, shouldn't be cleared, because this is the setting that ensures you get notifications for discussions you're participating in or when you are mentioned. Similarly, D, Watching, should not be cleared because it pertains to your chosen subscriptions, not automatic ones.
upvoted 1 times

RonZhong 1 year, 5 months ago
Selected Answer: BC
B is correct:

If you don't want notifications to be sent to your email, deselect email for participating and watching notifications.
upvoted 2 times

AlexeyG 1 year, 6 months ago
got this in 02 March 2023 exams. scored 870 marks.
upvoted 4 times

lugia4000 1 year, 7 months ago
By the way this came out today, picked B and D and had 930
upvoted 2 times

lugia4000 1 year, 7 months ago
Typo sorry, A and C
upvoted 4 times

smariussorin 1 year, 7 months ago
Selected Answer: AB
You receive a notification when an entry is made to any team discussion. - Automatically watch teams (A)

You need to ensure that you receive email notifications only for discussions in which you commented or in which you are mentioned. - Participating (B)

Seams that the question have changed order.
upvoted 2 times

SayCloud 1 year, 7 months ago
Selected Answer: AC
A C should be the correct answer, participating notification is desired.
https://docs.github.com/en/account-and-profile/managing-subscriptions-and-notifications-on-github/setting-up-notifications/about-notifications
upvoted 4 times

Frefren 1 year, 8 months ago
Selected Answer: AD
A and D in my opinion.

The question is about not receiving notifications for discussions, not repositories. By removing "Automatically watch teams" you opt-out of team @mentions. But, if the option was enabled until now, you will still receive notifications from past discussions, so you need to clear "Watching" as well. Option B "Participating" means that you either responded or are mentioned by someone in the particular discussion. The question clearly states that we still want to receive those notifications.

upvoted 3 times

ttl 1 year, 8 months ago

i will select AC

upvoted 1 times

Question #1 *Topic 6*

Your company has 60 developers who are assigned to four teams. Each team has 15 members.
The company uses an agile development methodology.
You need to structure the work of the development teams so that each team owns their respective work while working together to reach a common goal.
Which parts of the taxonomy should you enable the team to perform autonomously?

A. Features and Tasks

B. Initiatives and Epics

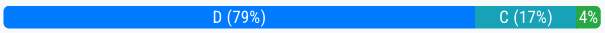
C. Epics and Features

D. Stories and Tasks

Suggested Answer: *A*
A feature typically represents a shippable component of software.
Features, examples:
➪ Add view options to the new work hub
➪ Add mobile shopping cart
➪ Support text alerts
➪ Refresh the web portal with new look and feel
User Stories and Tasks are used to track work. Teams can choose how they track bugs, either as requirements or as tasks
Incorrect Answers:
B, C: An epic represents a business initiative to be accomplished.
Epics, examples:
➪ Increase customer engagement
➪ Improve and simplify the user experience
➪ Implement new architecture to improve performance
➪ Engineer the application to support future growth
➪ Support integration with external services

Support mobile apps -
▪
Reference:
https://docs.microsoft.com/en-us/azure/devops/boards/backlogs/define-features-epics https://docs.microsoft.com/en-us/azure/devops/boards/work-items/about-work-items

Community vote distribution



alexax578 Highly Voted 2 years ago

Selected Answer: D

Epics consist of Features, which consist of User Stories, which consist of Tasks.
We want them to work together (on Epics and Features) and enable them to work autonomously (on User Stories and Tasks).
upvoted 27 times

Def21 2 years ago
Agree. By documentation
Scrum: Epic > Feature > Product backlog item > Task
Agile (including Scrum): Epic > Feature > User story > Task
https://docs.microsoft.com/en-us/azure/devops/boards/work-items/guidance/choose-process?view=azure-devops&tabs=agile-process

Thus, the answer is either Story/Task or Item/Task
upvoted 8 times

giuliohome 2 years ago
In Agile Scrum we have epic->user story->task, e.g. read https://adaptmethodology.com/epic-user-story-task/ In this case the question speak about agile therefore we want user stories (from the link above: User stories are regarded as the “heart of Scrum” because they serve as the

'building blocks' of the sprint), hence answer is D and neither features (A or C) nor initiatives (B)
upvoted 1 times

warchoon 1 year, 9 months ago
Not in MS Scrum workflow :)
https://learn.microsoft.com/en-us/azure/devops/boards/work-items/guidance/scrum-process-workflow?view=azure-devops
upvoted 2 times

cam9 Highly Voted 1 year, 6 months ago
Selected Answer: C
Everybody got this wrong - is C based on https://learn.microsoft.com/en-us/devops/plan/scaling-agile#line-of-autonomy
upvoted 5 times

gerardjongh 5 months ago
it is D, read the "Line of autonomy " in your link carefully. Epics and Features owned by Management while dev teams own the stories and tasks.
upvoted 3 times

vsvaid Most Recent 9 months ago
Selected Answer: D
User stories and tasks
upvoted 1 times

yana_b 1 year ago
Selected Answer: D
Stories and tasks
evidenced in the link provided by cam9:
https://learn.microsoft.com/en-us/devops/plan/scaling-agile#line-of-autonomy
upvoted 4 times

PrinceKumar 1 year, 1 month ago
Stories and Tasks
upvoted 2 times

ieboaix 1 year, 1 month ago
it is D, read the "Line of autonomy " of the link https://learn.microsoft.com/en-us/devops/plan/scaling-agile#line-of-autonomy. Epics and Features owns by Management while dev teams own the stories and tasks.
upvoted 5 times

renzoku 1 year, 1 month ago
Selected Answer: D
Epic > Feature > Stories > Task
Developers works on Stories and develop Tasks daily
upvoted 1 times

resonant 1 year, 1 month ago
Selected Answer: C
I think it's C. The common goals are the Epics, which are achieved through features. A team owns an epic and then the team splits the epic into features so that each member of the team can work on something different at the same time.
upvoted 2 times

xRiot007 1 year, 1 month ago
Correct answer is C - Epics and Features. Why ?
A - Features and Tasks - while features and tasks are part of agile, this granularity is TOO small for organizing multiple teams
B - Initiatives and Epics - granularity is too large. Initiatives are usually managed by program managers, not teams.
D - Stories and tasks - granularity is too small. This combo is usually done withing one team for an interation.
upvoted 2 times

renzoku 1 year, 2 months ago
Selected Answer: C
to enable the teams to perform autonomously work while working to a common goal, I think Epic -> Feature
For lower lever like specific work for developers could be Stories -> Task
upvoted 1 times

victorf_16 1 year, 4 months ago

Accoding to my perspective and knowledge and also validate with chatgpt the answer should be

C. Epics and Features

upvoted 2 times

Mcelona 1 year, 6 months ago

Selected Answer: D

I Think D

upvoted 1 times

Yatoom 1 year, 10 months ago

Selected Answer: B

I would suggest answer B: Initiatives and Epics.

- Initiatives are collections of epics that drive toward a common goal.
- An initiative compiles epics from multiple teams.

Source: https://www.atlassian.com/agile/project-management/epics-stories-themes

upvoted 2 times

liuliangzhou 2 years ago

Selected Answer: D

A user story is a tool used in Agile software development.

upvoted 4 times

Question #2 *Topic 6*

Your company creates a new Azure DevOps team.
You plan to use Azure DevOps for sprint planning.
You need to visualize the flow of your work by using an agile methodology.
Which Azure DevOps component should you use?

A. Kanban boards

B. sprint planning

C. delivery plans

D. portfolio backlogs

Suggested Answer: *A*
Customizing Kanban boards.
To maximize a team's ability to consistently deliver high quality software, Kanban emphasize two main practices. The first, visualize the flow of work, requires you to map your team's workflow stages and configure your Kanban board to match. Your Kanban board turns your backlog into an interactive signboard, providing a visual flow of work.
Reference:
https://azuredevopslabs.com/labs/azuredevops/agile/

Community vote distribution

A (100%)

27close Highly Voted 3 years, 10 months ago
Kanban boards and Taskboards support visualizing the flow of work and monitoring metrics to optimize that flow.
https://docs.microsoft.com/en-us/azure/devops/boards/boards/kanban-basics?view=azure-devops.
Kanban is the answer
upvoted 28 times

kumardeb Highly Voted 3 years, 10 months ago
A. Kanban boards
upvoted 9 times

vsvaid Most Recent 9 months ago
Selected Answer: A
Agree with answer
A
upvoted 1 times

yana_b 1 year ago
Selected Answer: A
Kanban boards
upvoted 1 times

CodeMaestro 1 year, 8 months ago
Selected Answer: A
When it comes to monitoring flow best to use kanban boards and taskboards is what my mother always said, 😂😂😂😂😂
upvoted 5 times

syu31svc 2 years, 1 month ago
Selected Answer: A
https://docs.microsoft.com/en-us/azure/devops/boards/boards/kanban-basics?view=azure-devops&viewFallbackFrom=azure-devops.

"As with most Agile practices, Kanban encourages monitoring key metrics to fine tune your processes"

Answer is A
upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: A

correct

upvoted 2 times

awron_durat 2 years, 7 months ago

Selected Answer: A

Kanban because of the keywords "visualize the flow"

upvoted 2 times

CodePoet 2 years, 8 months ago

Selected Answer: A

Excellently correct!

upvoted 2 times

Aniruddha_dravyakar 2 years, 11 months ago

Kanban boards is correct

upvoted 1 times

goatlord 3 years, 1 month ago

This is the right answer.

upvoted 3 times

Miles19 3 years, 5 months ago

Correct.

upvoted 4 times

27close 3 years, 10 months ago

The first, visualize the flow of work, requires you to map your team's workflow stages and configure your Kanban board to match.

upvoted 3 times

Question #3 *Topic 6*

Your company implements an Agile development methodology.
You plan to implement retrospectives at the end of each sprint.
Which three questions should you include? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Who performed well?

B. Who should have performed better?

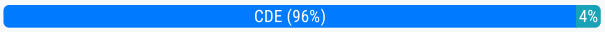
C. What could have gone better?

D. What went well?

E. What should we try next?

Suggested Answer: *BCE*
Sprint retrospective meetings -
The sprint retrospective meeting typically occurs on the last day of the sprint, after the sprint review meeting. In this meeting, your team explores its execution of
Scrum and what might need tweaking.
Based on discussions, your team might decide to change one or more processes to improve its own effectiveness, productivity, quality, and satisfaction. This meeting and the resulting improvements are critical to the agile principle of self-organization.
Look to address these areas during your team sprint retrospectives:
➪ Issues that affected your team's general effectiveness, productivity, and quality.
➪ Elements that impacted your team's overall satisfaction and project flow.
➪ What happened to cause incomplete backlog items? What actions will the team take to prevent these issues in the future?
Reference:
https://docs.microsoft.com/en-us/azure/devops/boards/sprints/best-practices-scrum

Community vote distribution



eray95 Highly Voted 3 years, 10 months ago
Correction C,D,E should be correct answers
upvoted 106 times

UnknowMan 2 years, 4 months ago
Yes always stay positive
upvoted 1 times

SriLen 3 years, 7 months ago
Correct , CDE
During the Sprint Retrospective, the team discusses:

What went well in the Sprint
What could be improved
What will we commit to improve in the next Sprint
https://www.scrum.org/resources/what-is-a-sprint-retrospective
upvoted 19 times

rdemontis 2 years, 5 months ago
thanks for sharing the article
upvoted 1 times

Geetesh05 2 years, 1 month ago
yea instead of who did this? who slacked? who screwed up?
retro and reflection, not finger pointing session
upvoted 7 times

kumardeb Highly Voted 3 years, 10 months ago

C. What could have gone better?
D. What went well?
E. What should we try next?
upvoted 15 times

UrbanRellik Most Recent 3 months, 3 weeks ago
Selected Answer: CDE
Blame-free retrospectives & Just a culture.

CDE
upvoted 2 times

ozbonny 6 months, 3 weeks ago
Selected Answer: CDE
C. What could have gone better?
D. What went well?
E. What should we try next?
upvoted 2 times

vsvaid 9 months ago
Selected Answer: CDE
C,D and E
upvoted 2 times

yana_b 1 year ago
Selected Answer: CDE
It is clearly stated in the link provided by SriLen
https://www.scrum.org/resources/what-is-a-sprint-retrospective
upvoted 3 times

renzoku 1 year, 1 month ago
Selected Answer: CD
Not Who else What
upvoted 2 times

xRiot007 1 year, 1 month ago
Retrospective NEVER focus on individuals, they always focus on the WHAT. What went well, what could have been done better, what do we want to try next, what do we want to do less, what do we want to stop doing or avoid doing and so on. So A annd B are automatically excluded, leaving C,D,E.
upvoted 3 times

vg30101981 1 year, 11 months ago
Selected Answer: CDE
CDE is the right Answer for sure.
During the Sprint Retrospective, the team discusses:

What went well in the Sprint
What could be improved
What will we commit to improve in the next Sprint

https://www.scrum.org/resources/what-is-a-sprint-retrospective
upvoted 6 times

syu31svc 2 years, 1 month ago
Selected Answer: CDE
CDE for sure

It's the process that we are looking at and not the individuals
upvoted 2 times

deltarj 2 years, 3 months ago
its "WHAT" rather than "WHO" in Agile...
upvoted 8 times

Eltooth 2 years, 4 months ago

Selected Answer: CDE

CDE are correct.

upvoted 3 times

pandrer 2 years, 4 months ago

Selected Answer: CDE

in the retrospective the questions are what? not who?

upvoted 4 times

UnknowMan 2 years, 4 months ago

Selected Answer: CDE

C,D,E is correct

upvoted 3 times

adamsw 2 years, 5 months ago

Selected Answer: CDE

CDE is the proper one

upvoted 3 times

rdemontis 2 years, 5 months ago

Selected Answer: CDE

The correct answer is CDE

https://www.scrum.org/resources/what-is-a-sprint-retrospective

upvoted 3 times

cannibalcorpse 2 years, 7 months ago

Selected Answer: CDE

not about who

upvoted 4 times

Question #4 *Topic 6*

Your team uses an agile development approach.
You need to recommend a branching strategy for the team's Git repository. The strategy must meet the following requirements.
- ✑ Provide the ability to work on multiple independent tasks in parallel.
- ✑ Ensure that checked-in code remains in a releasable state always.
- ✑ Ensure that new features can be abandoned at any time.
- ✑ Encourage experimentation.

What should you recommend?

A. a single long-running branch without forking

B. multiple long-running branches

C. a single fork per team member

D. a single long-running branch with multiple short-lived feature branches

Suggested Answer: *D*
Topic/feature branches, however, are useful in projects of any size. A topic branch is a short-lived branch that you create and use for a single particular feature or related work. This is something you've likely never done with a VCS before because it's generally too expensive to create and merge branches. But in Git it's common to create, work on, merge, and delete branches several times a day.
Reference:
https://git-scm.com/book/en/v2/Git-Branching-Branching-Workflows

Community vote distribution

D (100%)

denisred Highly Voted 3 years, 5 months ago
correct!
upvoted 21 times

Miles19 Highly Voted 3 years, 5 months ago
correct.
upvoted 7 times

Miten94 Most Recent 2 months, 3 weeks ago
Came in Exam June 23, 2024
upvoted 1 times

resonant 1 year ago
I didn't get this question on my exam on September 12, 2023, but I did get another that was very similar. It asked something about what to use when working in a new feature and the answers were short-lived feature branches.
upvoted 3 times

yana_b 1 year ago
Selected Answer: D
One long running main branch and short lived feature branches
upvoted 1 times

xRiot007 1 year, 1 month ago
D - long running branch with small feature branches. Why ?
If we need to abandon features, we can easily do so by deleting unwanted branches.
When something breaks (and it will, 100%) it will be on the feature branch, not the main.
upvoted 2 times

ShivaUdari 1 year, 7 months ago
Selected Answer: D
Correct
upvoted 1 times

ehurfheiz 1 year, 11 months ago
Selected Answer: D

Correct

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: D

"new features can be abandoned at any time"

I would take D based on this

upvoted 1 times

Eltooth 2 years, 3 months ago

Selected Answer: D

D is correct answer.

upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct, Aka Github flow

upvoted 2 times

rdemontis 2 years, 5 months ago

Selected Answer: D

correct answer

upvoted 1 times

Aniruddha_dravyakar 2 years, 11 months ago

D. a single long-running branch with multiple short-lived feature branches

upvoted 2 times

ScreamingHand 3 years, 1 month ago

Common sense really

upvoted 2 times

Question #5 *Topic 6*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You integrate a cloud-hosted Jenkins server and a new Azure DevOps deployment.
You need Azure DevOps to send a notification to Jenkins when a developer commits changes to a branch in Azure Repos.
Solution: You create a service hook subscription that uses the build completed event.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
You can create a service hook for Azure DevOps Services and TFS with Jenkins.
However, the service subscription event should use the code pushed event, is triggered when the code is pushed to a Git repository.

Community vote distribution
B (100%)

dimitartachev23 Highly Voted 3 years, 5 months ago
The answer is "NO", because the event should be when code is pushed and not when a build is completed.
upvoted 35 times

Optimist_Indian Highly Voted 2 years, 7 months ago
Got this question in Feb-2022 exam. Answer is : Code Push event.
upvoted 8 times

vsvaid Most Recent 9 months ago
Selected Answer: B
Agree with answer
upvoted 1 times

yana_b 1 year ago
Selected Answer: B
Correct answer
upvoted 1 times

WH16 1 year ago
Selected Answer: B
On exam 2023-09-06, selected B. No
upvoted 2 times

itexamsmicrosoft 1 year, 1 month ago
Selected Answer: B
B. No

Explanation:

The "build completed" event in Azure DevOps is triggered when a build pipeline run is completed, not when a developer commits changes to a branch in Azure Repos.

To achieve the goal of sending a notification to Jenkins when a developer commits changes to a branch in Azure Repos, a service hook subscription needs to be created that uses the code push event or the pull request created event.

Therefore, creating a service hook subscription that uses the "build completed" event would not meet the goal.
upvoted 2 times

xRiot007 1 year, 1 month ago

Well, this depends on how "lax" Microsoft sees the "commit" action. If it's just a commit done locally, on some random branch, it will not trigger Jenkins. If you push your code to origin or prepare PR, that will trigger Jenkins. Here is ref: https://learn.microsoft.com/en-us/azure/devops/service-hooks/overview?view=azure-devops

upvoted 1 times

CodeMaestro 1 year, 8 months ago

The answer is NO. You can read up on the same from the below link: https://learn.microsoft.com/en-us/azure/devops/service-hooks/overview?view=azure-devops

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: B

https://docs.microsoft.com/en-us/azure/devops/service-hooks/services/jenkins?view=azure-devops:

"You can trigger a Jenkins build when you push code to your project's Git repository"

Answer is No

upvoted 3 times

rdemontis 2 years, 5 months ago

Selected Answer: B

correct answer

upvoted 2 times

swapmaverick 2 years, 8 months ago

Question is - You need Azure DevOps to send a notification to Jenkins when a developer commits changes to a branch in Azure Repos.
- Clearly scenario is Code pushed not build completed so answer should be No
as given solution says - You create a service hook subscription that uses the build completed event.

upvoted 2 times

Aniruddha_dravyakar 2 years, 11 months ago

Given answer is correct as it is for branch

upvoted 1 times

Kalaismile06 3 years, 3 months ago

In addition to that the code pushed event available in the trigger type, please refer the below link for more info,
https://docs.microsoft.com/en-us/azure/devops/service-hooks/services/jenkins?view=azure-devops

upvoted 2 times

Kalaismile06 3 years, 3 months ago

The answer is "Yes". If you want to confirm, please refer the below link,
https://docs.microsoft.com/en-us/azure/devops/service-hooks/services/jenkins?view=azure-devops

If there is any changes in the code repo, the service hooks can be triggered for Java/any app.

upvoted 2 times

rafapaz09 3 years, 5 months ago

Doing a commit is not equal to doing a push, the documentation says "You can trigger a Jenkins build when you push code to your project's Git repository", that's it pushing your code into Git, not just committing your code

upvoted 1 times

Boruc 3 years, 5 months ago

The answer is "yes". There is a service hook with push code type of event as in the documentation: https://docs.microsoft.com/en-us/azure/devops/service-hooks/services/jenkins?view=azure-devops

upvoted 1 times

denisred 3 years, 5 months ago

Answer is Yes, the description is right!

upvoted 1 times

vasonic 3 years, 5 months ago

But the description also says that the event should be "code pushed", not "build completed", so that's why the answer is "No".

upvoted 8 times

noussa 3 years, 4 months ago

I agree , the answer is NO

upvoted 3 times

Question #6 *Topic 6*

You have a project in Azure DevOps that has a release pipeline.
You need to integrate work item tracking and an Agile project management system to meet the following requirements:
➪ Ensure that developers can track whether their commits are deployed to production.
➪ Report the deployment status.
➪ Minimize integration effort.
Which system should you use?

A. Asana

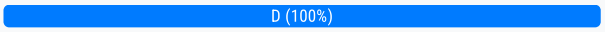
B. Basecamp

C. Trello

D. Jira

Suggested Answer: *D*
Jira Software is a development tool used by agile teams to plan, track, and manage software releases. Using Azure Pipelines, teams can configure CI/CD pipelines for applications of any language, deploying to any platform or any cloud.
Note: Microsoft and Atlassian have partnered together to build an integration between Azure Pipelines and Jira Software.
This integration connects the two products, providing full tracking of how and when the value envisioned with an issue is delivered to end users. This enables teams to setup a tight development cycle from issue creation through release. Key development milestones like builds and deployments associated to a Jira issue can then be tracked from within Jira Software.
Incorrect Answers:
C: Trello is a collaboration tool that organizes your projects into boards. In one glance, Trello tells you what's being worked on, who's working on what, and where something is in a process.
Reference:
https://devblogs.microsoft.com/devops/azure-pipelines-integration-with-jira-software/

Community vote distribution



vsvaid 9 months ago
Selected Answer: D
Agree with answer
upvoted 2 times

xRiot007 1 year, 1 month ago
D - JIRA will help you manage deployments and is integrated with Azure Pipelines.
upvoted 3 times

ShivaUdari 1 year, 7 months ago
Selected Answer: D
D is correct
upvoted 1 times

CodeMaestro 1 year, 8 months ago
Provided answer is correct, the question deals with both intergration and deployment and JIRA is a good candidate in that regard.
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: D
The #1 software development tool used by agile teams

As per Jira website

Answer is D
upvoted 4 times

Eltooth 2 years, 3 months ago
Selected Answer: D

D is correct answer.

Jira boards

upvoted 1 times

Exam_pas 2 years, 4 months ago

Provided answer is correct !

https://www.atlassian.com/software/jira/guides/use-cases/what-is-jira-used-for#jira-for-agile-teams

upvoted 1 times

Question #7 *Topic 6*

You plan to onboard 10 new developers.
You need to recommend a development environment that meets the following requirements:
➪ Integrates with GitHub
➪ Provides integrated debugging tools
➪ Supports remote workers and hot-desking environments
➪ Supports developers who use browsers, tablets, and Chromebooks
What should you recommend?

A. VS Code

B. Xamarin Studio

C. MonoDevelop

D. Github Codespaces

Suggested Answer: *D*
You can develop in your codespace directly in Visual Studio Code by connecting the GitHub Codespaces extension with your account on GitHub.
Reference:
https://docs.github.com/en/codespaces/developing-in-codespaces/using-codespaces-in-visual-studio-code

Community vote distribution
D (100%)

xRiot007 1 year, 1 month ago
The answer is D - GitHub codespace.
What I would recommend in real life is to not enforce this for your remote workers because they usually have their own setups in place that work for them, so unless there are some super strong reasons for using codespaces, don't.
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: D
https://devblogs.microsoft.com/visualstudio/visual-studio-codespaces-is-consolidating-into-github-codespaces/
https://code.visualstudio.com/docs/remote/remote-overview

Answer is D
upvoted 2 times

Eltooth 2 years, 3 months ago
Selected Answer: D
D is correct answer.
upvoted 1 times

UnknowMan 2 years, 4 months ago
Because " Supports remote workers and hot-desking environments"
The github codespaces do the job
upvoted 1 times

jay158 2 years, 4 months ago
Selected Answer: D
https://docs.github.com/en/codespaces
upvoted 3 times

Question #8 *Topic 6*

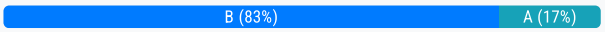
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You integrate a cloud-hosted Jenkins server and a new Azure DevOps deployment.
You need Azure DevOps to send a notification to Jenkins when a developer commits changes to a branch in Azure Repos.
Solution: You create an email subscription to an Azure DevOps notification.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
You can create a service hook for Azure DevOps Services and TFS with Jenkins.
Reference:
https://docs.microsoft.com/en-us/azure/devops/service-hooks/services/jenkins

Community vote distribution



Abhishek81 Highly Voted 4 years, 2 months ago
The answer written is correct. As tou have to create webhook. Follow the link which is given in the answer
upvoted 10 times

jacyang Highly Voted 4 years, 2 months ago
Service Hook
upvoted 9 times

CodeMaestro 1 year, 8 months ago
Service Hooks support: Build Completed, Code Pushed, Pull Request merge Completed and Release Deployment completed events in the use of Jenkins and even with that it is in regard to trigger generic build and trigger guild build actions.
upvoted 1 times

Pamban Most Recent 1 year, 2 months ago
this series of yes/no question appeared on today's (20/06/23) exam.selected the given answer in examtopics.
Correct answer is service hook which uses code push event

scored 955. should be correct! cheers
upvoted 4 times

syu31svc 2 years, 1 month ago
Selected Answer: B
Answer is B

https://docs.microsoft.com/en-us/azure/devops/service-hooks/services/jenkins?view=azure-devops:

"You can trigger a Jenkins build when you push code to your project's Git repository"
upvoted 2 times

Eltooth 2 years, 3 months ago
Selected Answer: B
B is correct answer.
upvoted 2 times

rdemontis 2 years, 5 months ago
Selected Answer: B
answer is correct. you need a service hook

upvoted 2 times

jonasis 2 years, 6 months ago

Selected Answer: B

Email subscription doesn't send to Jenkins. You need webhook

upvoted 2 times

testuser_444 2 years, 6 months ago

Selected Answer: B

correct

upvoted 2 times

[Removed] 2 years, 9 months ago

Selected Answer: A

voting for a correct answer A

upvoted 2 times

[Removed] 2 years, 9 months ago

this was meant for previous question, here answer is B.

upvoted 2 times

Aniruddha_dravyakar 2 years, 11 months ago

Given answer is correct as it is for branch

upvoted 1 times

SuperPetey 3 years, 3 months ago

Answer should be yes - of course MSFT's own platform supports this.
https://docs.microsoft.com/en-us/azure/devops/notifications/manage-your-personal-notifications?view=azure-devops&tabs=new-account-enabled

upvoted 2 times

jvyas 2 years, 5 months ago

Here you have to trigger Jenkins pipeline, email if for personal notification it wont trigger jenkins.

upvoted 1 times

xRiot007 1 year, 1 month ago

You need to *trigger* Jenkins first. For that you need a service hook that will support one of the following events: Build completed, code pushed, PR merge attempted, release deployment completed. Ref https://learn.microsoft.com/en-us/azure/devops/service-hooks/overview?view=azure-devops

upvoted 1 times

NKnab 4 years, 1 month ago

Create a service hook so that after a code commit, jenkins job can start

upvoted 5 times

ddmoto 4 years, 2 months ago

Does Anyone know the right answer to this

upvoted 2 times

ukohae39 3 years, 2 months ago

Solution:
You integrate a cloud-hosted Jenkins server and a new Azure DevOps deployment.
You need Azure DevOps to send a notification to Jenkins when a developer commits changes to a branch in Azure Repos.
Solution: You create a service hook subscription that uses the code pushed event.

upvoted 2 times

Question #9 *Topic 6*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You integrate a cloud-hosted Jenkins server and a new Azure DevOps deployment.
You need Azure DevOps to send a notification to Jenkins when a developer commits changes to a branch in Azure Repos.
Solution: You create a service hook subscription that uses the code pushed event.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
You can create a service hook for Azure DevOps Services and TFS with Jenkins.
The code push event is triggered when the code is pushed to a Git repository.
Reference:
https://docs.microsoft.com/en-us/azure/devops/service-hooks/services/jenkins https://docs.microsoft.com/en-us/azure/devops/service-hooks/events

Community vote distribution
A (100%)

erique4846 Highly Voted 3 years, 4 months ago
correct, verified
upvoted 9 times

Pamban Most Recent 1 year, 2 months ago
this series of yes/no question appeared on today's (20/06/23) exam.selected the given answer in examtopics.
Correct answer is service hook which uses code push event

scored 955. should be correct! cheers
upvoted 2 times

syu31svc 2 years, 1 month ago
Selected Answer: A
https://docs.microsoft.com/en-us/azure/devops/service-hooks/services/jenkins?view=azure-devops:

"You can trigger a Jenkins build when you push code to your project's Git repository"

Answer is yes
upvoted 1 times

Eltooth 2 years, 3 months ago
Selected Answer: A
A is correct answer.
upvoted 2 times

UnknowMan 2 years, 4 months ago
Correct
upvoted 1 times

rdemontis 2 years, 5 months ago
Selected Answer: A
this is the answer to this solution based scenario
upvoted 2 times

swapmaverick 2 years, 8 months ago

Right answer - Code pushed event

upvoted 1 times

Aniruddha_dravyakar 2 years, 11 months ago

Given answer is correct as it is for branch

upvoted 1 times

Kalaismile06 3 years, 3 months ago

yes, service hook trigger an event and we can configure notification

upvoted 4 times

vglearn 3 years, 7 months ago

Yes, Correct answer

upvoted 3 times

27close 3 years, 10 months ago

yes service hook

upvoted 4 times

Question #10 *Topic 6*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You integrate a cloud-hosted Jenkins server and a new Azure DevOps deployment.
You need Azure DevOps to send a notification to Jenkins when a developer commits changes to a branch in Azure Repos.
Solution: You add a trigger to the build pipeline.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
You can create a service hook for Azure DevOps Services and TFS with Jenkins.
Reference:
https://docs.microsoft.com/en-us/azure/devops/service-hooks/services/jenkins

Community vote distribution
B (100%)

TateBytes Highly Voted 3 years, 7 months ago
No. Keep in mind this is about the notification to Jenkins that is sent after code is pushed to Azure repo.. this doesn't require the build pipeline trigger. Moreover, the build trigger is not in Azure Repo. The build is triggered in Jenkins, hence you would not need to add a trigger to the Jenkins build pipeline to send a notification to itself.
upvoted 20 times

rdemontis 2 years, 5 months ago
thanks for explanation
upvoted 1 times

temporal111 Highly Voted 3 years, 12 months ago
It should be "yes", a build pipeline trigger can invoke 3rd party services.
upvoted 5 times

buzzerboy 1 year, 7 months ago
that's what I thought too. Pretty sure it would work. But I guess its not the best practice.
upvoted 1 times

Pamban Most Recent 1 year, 2 months ago
this series of yes/no question appeared on today's (20/06/23) exam.selected the given answer in examtopics.
Correct answer is service hook which uses code push event

scored 955. should be correct! cheers
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: B
https://docs.microsoft.com/en-us/azure/devops/service-hooks/services/jenkins?view=azure-devops:

"You can trigger a Jenkins build when you push code to your project's Git repository"

Answer is No
upvoted 3 times

Eltooth 2 years, 3 months ago
Selected Answer: B
B is correct answer.

upvoted 2 times

rdemontis 2 years, 5 months ago

Selected Answer: B

correct answer

upvoted 2 times

moota 3 years, 2 months ago

The solution is badly worded so it generates confusion

upvoted 1 times

Kalaismile06 3 years, 3 months ago

Repeated question, the ans is No. Shared the link as well

upvoted 2 times

piyipo3349 3 years, 8 months ago

I believe the answer is YES:

1- One way is to run CI jobs in Jenkins separately
2- The alternate way is to wrap a Jenkins CI job inside an Azure pipeline <--
source: https://azuredevopslabs.com/labs/vstsextend/jenkins/

upvoted 2 times

hgx32983 3 years, 4 months ago

When will you understand that we don't care what you believe to be true.
Please if you're not sure about something, don't comment.
The answer is definitly NO.
As mentioned, one wants to send a notification to jenkins when a commit occurs in order to run the build pipeline on the jenkins.

upvoted 6 times

ScreamingHand 3 years, 1 month ago

No need for aggression. Anyone should feel free to discuss whatever, - if you're not interested in their comment, don't comment

upvoted 3 times

cherry22 3 years, 8 months ago

The answer is correct.
In build pipeline, you have to 'Enable continuous integration' in trigger, not 'Adding' trigger.

upvoted 5 times

Dady9 3 years, 9 months ago

you don't have build in DevOps only repo - commits changes to a branch.
You can trigger a Jenkins build when you push code to your project's Git repository or when you check in code to Team Foundation version control.
https://docs.microsoft.com/en-us/azure/devops/service-hooks/services/jenkins?view=azure-devops#trigger-jenkins
So answer - No

upvoted 2 times

27close 3 years, 10 months ago

Next, we need to enable the “Generic Webhook Trigger” under the “Build Triggers” section. We need to add a “Post content parameter” with the same expression we determined earlier from our JSONPath Expression Tester. The result will be stored in the “branch” variable. Next, we need to add a filter which lets us know if the branch that was pushed to is the branch we were looking for
-answer is yes -possible

upvoted 1 times

Question #11 *Topic 6*

You plan to create in Azure DevOps. Multiple developers will work on the project. The developers will work offline frequently and will require access to the full project history while they are offline.
Which version control solution should you use?

A. Team Foundation Version Control

B. Git

C. TortoiseSVN

D. Subversion

Suggested Answer: *B*
Git history: File history is replicated on the client dev machine and can be viewed even when not connected to the server. You can view history in Visual Studio and on the web portal.
Note: Azure Repos supports two types of version control: Git and Team Foundation Version Control (TFVC).
Incorrect Answers:
A: Team Foundation Version Control: File history is not replicated on the client dev machine and so can be viewed only when you're connected to the server.
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/tfvc/comparison-git-tfvc

Community vote distribution
B (100%)

kumardeb Highly Voted 3 years, 10 months ago
B. Git
upvoted 9 times

DevopsRock Most Recent 1 week, 1 day ago
Selected Answer: B
Git, just need to sync once
upvoted 1 times

ozbonny 6 months, 3 weeks ago
Selected Answer: B
B since A is for remote only
upvoted 1 times

xRiot007 1 year, 1 month ago
B - Git will provide offline history. You can use GitHub Extensions to see this history in a more human friendly way.
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: B
B for sure
upvoted 1 times

Eltooth 2 years, 4 months ago
Selected Answer: B
B is correct answer.
upvoted 1 times

UnknowMan 2 years, 4 months ago
Offline working -> Git
upvoted 3 times

rdemontis 2 years, 5 months ago
Selected Answer: B
correct answer
upvoted 1 times

MikeHugeNerd 2 years, 9 months ago
As correct as correct can ever be.
upvoted 1 times

Kalaismile06 3 years, 3 months ago
Git...
upvoted 4 times

eray95 3 years, 10 months ago
Given ans is correct
upvoted 4 times

Hooters 3 years, 10 months ago
Agree, given answer is correct
upvoted 2 times

sidharthwader 2 years, 8 months ago
agree! given answer is correct
upvoted 1 times

Skankhunt 1 month, 3 weeks ago
Agree, given answer is correct
upvoted 1 times

Question #12 *Topic 6*

You plan to onboard 10 new developers.
You need to recommend a development environment that meets the following requirements:
➪ Integrates with GitHub
➪ Provides integrated debugging tools
➪ Supports remote workers and hot-desking environments
➪ Supports developers who use browsers, tablets, and Chromebooks
What should you recommend?

A. VS Code

B. Xamarin Studio

C. MonoDevelop

D. Visual Studio Codespaces

Suggested Answer: *D*
Visual Studio Codespaces is built to accommodate the widest variety of projects or tasks, including GitHub and integrating debugging.
Visual Studio Codespaces conceptually and technically extends the Visual Studio Code Remote Development extensions.
In addition to "backend" environments, Visual Studio Codespaces supports these "frontend" editors:
➪ Visual Studio Code
➪ Visual Studio Code-based editor in the browser
Reference:
https://docs.microsoft.com/sv-se/visualstudio/codespaces/overview/what-is-vsonline

Community vote distribution
D (100%)

berkejf Highly Voted 3 years, 7 months ago
Answer is correct
upvoted 18 times

meera30 3 years, 2 months ago
This option was not in the exam today
upvoted 3 times

mann29 3 years, 2 months ago
then what other options are there
upvoted 2 times

Kolego 2 years, 11 months ago
The rest are the same. Answer is still GitHub Codespaces.
upvoted 3 times

llikethis 3 years, 2 months ago
Answer is GitHub Codespaces
upvoted 9 times

Infinity31 3 years, 2 months ago
which options do you had?
upvoted 1 times

nocap Highly Voted 3 years, 2 months ago
According to this link, Visual Studio Codespaces, is now GitHub Codespaces, so the answer is probably still D, but it will probably be labeled "GitHub Codespaces" now.
upvoted 7 times

friendlyvlad Most Recent 1 year, 9 months ago
I believe it is A. VS Code offers a debugger, remote work, and is browser-based.
upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: D
https://devblogs.microsoft.com/visualstudio/visual-studio-codespaces-is-consolidating-into-github-codespaces/
https://code.visualstudio.com/docs/remote/codespaces

Answer is GitHub Codespaces but in this case D is the correct choice
upvoted 1 times

JarJarJim 2 years, 2 months ago
Selected Answer: D
GitHub Codpaces is the correct answer
upvoted 2 times

Eltooth 2 years, 4 months ago
Selected Answer: D
D is correct answer.
upvoted 1 times

UnknowMan 2 years, 4 months ago
Correct
upvoted 1 times

Whirly 2 years, 5 months ago
Exam Question April 1st 2022 - GH Codespaces
upvoted 4 times

rdemontis 2 years, 5 months ago
Selected Answer: D
correct answer. Probably it should be changed to GitHub Codespaces
https://code.visualstudio.com/docs/remote/codespaces
https://devblogs.microsoft.com/visualstudio/visual-studio-codespaces-is-consolidating-into-github-codespaces/
upvoted 1 times

rdemontis 2 years, 5 months ago
I share another intersting article about GitHub Codespaces
https://code.visualstudio.com/api/advanced-topics/remote-extensions
upvoted 1 times

lugospod 2 years, 7 months ago
Got this January 2022. Git Codespaces is used now (100% on that part)
upvoted 1 times

Kolego 2 years, 11 months ago
The answer now is GitHub Codespaces
upvoted 2 times

nocap 3 years, 2 months ago
welp, forgot the link - forgot the link -
https://devblogs.microsoft.com/visualstudio/visual-studio-codespaces-is-consolidating-into-github-codespaces/
upvoted 5 times

rdemontis 2 years, 5 months ago
thanks for sharing the article
upvoted 1 times

itworxx 3 years, 2 months ago
VSCode:
➪ Integrates with GitHub
➪ Provides integrated debugging tools
➪ Supports remote workers and hot-desking environments
➪ Supports developers who use browsers, tablets, and Chromebooks
Does all that (tablet users: use browser).
More info: https://code.visualstudio.com/docs/remote/remote-overview
VSCode in a browser: open cloud shell in Azure Portal and type "code"
upvoted 5 times

sikor1994 3 years, 2 months ago

It's probably the correct answer. Today at the Microsoft Training VSCode was mentioned as the right tool. There is something like GitHub Codespaces but it has not been released yet.

upvoted 2 times

Question #13 *Topic 6*

You have a build pipeline in Azure Pipelines.
You create a Slack App Integration.
You need to send build notifications to a Slack channel named #Development.
What should you do first?

A. Create a project-level notification.

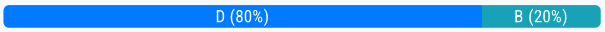
B. Configure a service connection.

C. Create a global notification.

D. Creates a service hook subscription.

Suggested Answer: *D*
Create a service hook for Azure DevOps with Slack to post messages to Slack in response to events in your Azure DevOps organization, such as completed builds, code changes, pull requests, releases, work items changes, and more.
Note:
1. Go to your project Service Hooks page:
https://{orgName}/{project_name}/_settings/serviceHooks
Select Create Subscription.
2. Choose the types of events you want to appear in your Slack channel.
3. Paste the Web Hook URL from the Slack integration that you created and select Finish.
4. Now, when the event you configured occurs in your project, a notification appears in your team's Slack channel.
Reference:
https://docs.microsoft.com/en-us/azure/devops/service-hooks/services/slack

Community vote distribution



Dalias Highly Voted 3 years, 2 months ago
Got this in 30 June 2021 exam. Scored 800+ the provided answer is correct - service hook sub. The question in the exam has one close one which is service connection configure
upvoted 22 times

jvyas 2 years, 5 months ago
Thank you, It is very easy to get mixed up.
upvoted 2 times

yana_b Most Recent 1 year ago
Selected Answer: D
Service hook is the correct answer, clearly described here https://learn.microsoft.com/en-us/azure/devops/service-hooks/services/slack?view=azure-devops
upvoted 3 times

xRiot007 1 year, 1 month ago
You don't need a service connection for this, just a service hook subscription. You will subscribe to publish build messages on specific URL (which is your slack service). A service connection is needed for other tasks, like building outside of Azure, when you tell for example GitHub Enterprise to build your project.
upvoted 1 times

Pamban 1 year, 3 months ago
Selected Answer: D
Answer is correct!

reference: https://docs.microsoft.com/en-us/azure/devops/service-hooks/services/slack?view=azure-devops:
upvoted 1 times

Shanmugamani 1 year, 3 months ago
I think given answer is correct because service connection is required at the time of release. Here for build notifications, configuring service connection may not be required.

upvoted 1 times

Fal991l 1 year, 5 months ago

Selected Answer: B

GPT: Yes, configuring a service connection (B) should be the first step to send build notifications to a Slack channel named #Development, followed by creating a service hook subscription that sends build notifications to the Slack channel via the Slack App Integration.

upvoted 2 times

Fal991l 1 year, 5 months ago

The service connection will provide Azure Pipelines with the necessary credentials and authentication information to communicate with the Slack App Integration. Once the service connection is established, you can create a service hook subscription in Azure Pipelines that triggers notifications to be sent to the Slack channel when a build completes.

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: D

https://docs.microsoft.com/en-us/azure/devops/service-hooks/services/slack?view=azure-devops:

"Now, when the event you configured occurs in your project, a notification appears in your team's Slack channel"

Answer is D

upvoted 2 times

Eltooth 2 years, 3 months ago

Selected Answer: D

D is correct answer.

upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 2 times

rdemontis 2 years, 5 months ago

Selected Answer: D

correct answer

upvoted 1 times

Booldozer 2 years, 12 months ago

Correct :)

upvoted 1 times

V_Ramon 3 years, 1 month ago

this question came out today, July 28, 2021

upvoted 4 times

erico 3 years, 2 months ago

You can also create a service hook subscription that connects to your Slack channel. Whenever an event occurs in the build pipeline, a notification can be sent onto the Slack channel.

upvoted 1 times

leonelferrari 3 years, 3 months ago

Correct!

upvoted 2 times

fihdsaHFHVKJFEV324 3 years, 6 months ago

Correct:
https://docs.microsoft.com/en-us/azure/devops/service-hooks/services/slack?view=azure-devops

upvoted 3 times

Question #14 *Topic 6*

You have an Azure DevOps organization named Contoso and an Azure subscription.
You use Azure DevOps to build and deploy a web app named App1. Azure Monitor is configured to generate an email notification in response to alerts generated whenever App1 generates a server-side error.
You need to receive notifications in Microsoft Teams whenever an Azure Monitor alert is generated.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Create an Azure Monitor workbook.

B. Create an Azure logic app that has an HTTP request trigger.

C. Create an Azure logic app that has an Azure DevOps trigger.

D. Modify an action group in Azure Monitor.

E. Modify the Diagnostics settings in Azure Monitor.

Suggested Answer: *BD*
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups-logic-app

Community vote distribution
BD (100%)

Marang73 Highly Voted 3 years, 10 months ago
Answers should be B and D. In Azure Monitor action group configure a webhook, the url of the webhook must be the url (trigger) of the Logic App. In the Logic App you can use the Team connector to send a message to a Teams channel
upvoted 52 times

d0bermannn 3 years ago
agreed with Morke, no need to webhook here
upvoted 1 times

yhredil 3 years, 10 months ago
You are right
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups-logic-app
upvoted 5 times

Morke 3 years, 8 months ago
You don't need to configure a Webhook. You configure it directly to call the Logic app, and in the Logic App you use an Http request as the trigger.
upvoted 7 times

kumardeb Highly Voted 3 years, 10 months ago
B. Create an Azure logic app that has an HTTP request trigger.
D. Modify an action group in Azure Monitor.
upvoted 19 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: BD
Correct B D
upvoted 1 times

ieboaix 1 year, 1 month ago
B and D, verified.
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: BD
Given link supports B and D very clearly
upvoted 1 times

Eltooth 2 years, 4 months ago

Selected Answer: BD

B and D are correct answers.

upvoted 2 times

UnknowMan 2 years, 4 months ago

Update the action group to call an Http trigger

Logic app is triggered by the action group and contact teams

upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: BD

Answer C is wrong. We need a logic app with an http request trigger

https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups-logic-app

upvoted 2 times

adone 2 years, 6 months ago

B and D looks the less worse answer but note that you can receive a message to any Teams channel via Webhook natively in Teams without the need of a logic apps. I would never use a logic apps for this purpose.

upvoted 1 times

xRiot007 1 year, 1 month ago

It depends on how human friendly you want to be. Logic Apps are designed to be easily understood by non tech people, like PMs, stakeholders, managers, etc. If you have such a requirement, logic apps will be better than webhooks.

upvoted 1 times

jonasis 2 years, 6 months ago

Selected Answer: BD

BD correct

upvoted 2 times

lugospod 2 years, 7 months ago

Got this January 2022. Went with BD

upvoted 2 times

Pankaj78 2 years, 9 months ago

Selected Answer: BD

Answers should be B and D

upvoted 1 times

AlMargoi 2 years, 9 months ago

Answers should be B and D. The amount of incorrect answers here is concerning.

upvoted 2 times

Gogu83 2 years, 9 months ago

Selected Answer: BD

I believe that this are correct goind through the documentation

upvoted 1 times

[Removed] 2 years, 9 months ago

Selected Answer: BD

BD correct

upvoted 1 times

GigaCaster 2 years, 10 months ago

The message needs to be generated when App1 gives a server-side error os C and D would be correct.

upvoted 1 times

combo_breaker 3 years, 6 months ago

It's B and D. I read over the reference URL that was attached to this question and they chose an AzureDevops Trigger based on checking in code which is correct in that situation. However, the question is based on an Azure Monitor alert which would be triggered from HTTP.

upvoted 6 times

Question #15 *Topic 6*

HOTSPOT -

Your company uses Azure DevOps for Git source control.

You have a project in Azure DevOps named Contoso App that contains the following repositories:

- https://dev.azure.com/contoso/contoso-app/core-api
- https://dev.azure.com/contoso/contoso-app/core-spa
- https://dev.azure.com/contoso/contoso-app/core-db

You need to ensure that developers receive Slack notifications when there are pull requests created for Contoso App.

What should you run in Slack? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

/azrepos

feedback
signin
subscribe
subscriptions

https://dev.azure.com/contoso/contoso-app
https://dev.azure.com/contoso/contoso-app/core-api
https://dev.azure.com/contoso/contoso-app/core-db
https://dev.azure.com/contoso/contoso-app/core-spa

Suggested Answer:

Answer Area

/azrepos

feedback
signin
subscribe
subscriptions

https://dev.azure.com/contoso/contoso-app
https://dev.azure.com/contoso/contoso-app/core-api
https://dev.azure.com/contoso/contoso-app/core-db
https://dev.azure.com/contoso/contoso-app/core-spa

Box 1: subscribe -

To start monitoring all Git repositories in a project, use the following slash command inside a channel:

/azrepos subscribe [project url]

Box 2: https://dev.azure.com/contoso/contoso-app

You can also monitor a specific repository using the following command:

/azrepos subscribe [repository url]

The repository URL can be to any page within your repository that has your repository name.

For example, for Git repositories, use:

/azrepos subscribe https://dev.azure.com/myorg/myproject/_git/myrepository

Reference:

https://docs.microsoft.com/en-us/azure/devops/repos/integrations/repos-slack

Dalias Highly Voted 3 years, 2 months ago

Got this in 30 June 2021 exam. Scored 800+ the provided answer is correct

upvoted 18 times

xRiot007 1 year, 1 month ago

You are lieing. When you finish the exam you get the EXACT score, not some range. or limit.

upvoted 1 times

pau23435775 2 years, 4 months ago

i wonder who are theses people who revisits the site just to comment they scored something!

upvoted 31 times

jvyas 2 years, 3 months ago

I was thinking the same.

upvoted 2 times

FunkyB 2 years, 3 months ago

Posers :-)
Seriously, I appreciate everyone that contributes with comments. I actually review all the links, and I truly learn the material. We are all learning and helping each other.
upvoted 15 times

shash_ank 2 years, 3 months ago
Yeah and why do they put score in '800+' and "910+' format?? If you have to comment your score, comment the exact score you got. Don't these people have their score report?
upvoted 7 times

Hgreg 9 months ago
Dude confirmed that at specified date the question was still a valid exam question. That is worth to know. I'd assume it is safer to give just a range instead of the exact score (no score at all would also be fine :-)).
A little bit of paranoia never hurts. What if he is the only person that got a specific score on that day and MS can somehow track him? :-D
upvoted 4 times

ozbonny Most Recent 6 months, 3 weeks ago
Correct Answer for me
upvoted 1 times

vsvaid 9 months ago
Subscribe and contoso-app
Agree with answer
upvoted 1 times

PeterLabelle 9 months, 1 week ago
Duplicate of Topic 2 Q 21
upvoted 1 times

syu31svc 2 years, 1 month ago
Given answer is correct and link provided supports it
upvoted 1 times

Eltooth 2 years, 4 months ago
Subscribe and /contoso-app
upvoted 2 times

UnknowMan 2 years, 4 months ago
Correct
upvoted 1 times

rdemontis 2 years, 5 months ago
correct
upvoted 2 times

Optimist_Indian 2 years, 7 months ago
Got this question in Feb-2022 exam (scored 910+). Given answer is correct.
upvoted 4 times

celciuz 3 years ago
This question came out, August 2021
upvoted 3 times

JerryGolais 3 years, 3 months ago
Seems correct.

Azure ReposAPP 11:06 PM
Here are some of the things you can do:
Subscribe to a repository or all repositories in a project to receive notifications
/azrepos subscribe [repository url/ project url]
Add or remove subscriptions for this channel
/azrepos subscriptions
upvoted 4 times

theboywonder 3 years, 4 months ago

Correctamundo dude

upvoted 4 times

Question #16 *Topic 6*

You have an Azure DevOps organization that contains a project named Project1.
You need to create a published wiki in Project1.
What should you do first?

A. Modify the Storage settings of Project1.

B. In Project1, create an Azure DevOps pipeline.

C. In Project1, create an Azure DevOps repository.

D. Modify the Team configuration settings of Project1.

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/devops/project/wiki/publish-repo-to-wiki?view=azure-devops&tabs=browser

Community vote distribution
C (100%)

ScreamingHand Highly Voted 3 years, 1 month ago
correctomundo cowabunga dudes
upvoted 26 times

d0bermannn 3 years ago
sorry to all, offtopp: 've been transported back in time to 80's with cowabunga
upvoted 7 times

[Removed] 2 years, 9 months ago
whenever i see correctomundo i see a good man!
upvoted 12 times

zellck Highly Voted 1 year, 3 months ago
Selected Answer: C
C is the answer.

https://learn.microsoft.com/en-us/azure/devops/project/wiki/wiki-create-repo?view=azure-devops&tabs=browser
Every team project can have a wiki. Use the wiki to share information with your team to understand and contribute to your project.

Each team project wiki is powered by a Git repository in the back-end. When you create a team project, a Wiki Git repo is not created by default. Provision a Git repository to store your wiki Markdown files, or publish existing Markdown files from a Git repository to a wiki.
upvoted 6 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: C
C. In Project1, create an Azure DevOps repository.
upvoted 1 times

vsvaid 9 months ago
Agree with answer
upvoted 1 times

xRiot007 1 year, 1 month ago
Answer is C - in Project1 you create a repository.
In Azure DevOps we have Organization > Project > Repo > code/docs/pipelines/other files
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: C
From given link:

"You must have enabled Azure Repos service for your project"

C for correct

upvoted 2 times

Redimido 2 years, 2 months ago

We do that at work. It's correct. The .md files have their versioning in the repo.

upvoted 3 times

Eltooth 2 years, 3 months ago

Selected Answer: C

C is correct answer.

upvoted 2 times

UnknowMan 2 years, 4 months ago

published wiki need a repository

upvoted 3 times

rdemontis 2 years, 5 months ago

Selected Answer: C

correct

upvoted 1 times

PrawinG 3 years, 2 months ago

Correct

upvoted 3 times

Question #17 *Topic 6*

Your company plans to use an agile approach to software development.
You need to recommend an application to provide communication between members of the development team who work in locations around the world. The applications must meet the following requirements:
➪ Provide the ability to isolate the members of different project teams into separate communication channels and to keep a history of the chats within those channels.
➪ Be available on Windows 10, Mac OS, iOS, and Android operating systems.
➪ Provide the ability to add external contractors and suppliers to projects.
➪ Integrate directly with Azure DevOps.
What should you recommend?

A. Microsoft Project

B. Bamboo

C. Microsoft Lync

D. Microsoft Teams

Suggested Answer: *D*
➪ Within each team, users can create different channels to organize their communications by topic. Each channel can include a couple of users or scale to thousands of users.
➪ Microsoft Teams works on Android, iOS, Mac and Windows systems and devices. It also works in Chrome, Firefox, Internet Explorer 11 and Microsoft Edge web browsers.
➪ The guest-access feature in Microsoft Teams allows users to invite people outside their organizations to join internal channels for messaging, meetings and file sharing. This capability helps to facilitate business-to-business project management.
➪ Teams integrates with Azure DevOps.
Note: Slack would also be a correct answer, but it is not an option here.
Reference:
https://searchunifiedcommunications.techtarget.com/definition/Microsoft-Teams

Community vote distribution

D (100%)

alce2020 Highly Voted 3 years, 5 months ago
answer is teams
upvoted 18 times

Akc0 1 year, 4 months ago
This and the "Github spaces" questions feel like MS product marketing ads rather than actual technical questions "hey do you know we can do this, you should sell our product" lol
upvoted 2 times

ScreamingHand Highly Voted 3 years, 1 month ago
Teams or Slack every time
upvoted 11 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: D
D. Microsoft Teams

it is funny this question Microsoft promoting Microsoft products
upvoted 1 times

vsvaid 9 months ago
Selected Answer: D
Agree with
upvoted 1 times

LGWJ12 1 year, 9 months ago
Selected Answer: D

D is the correct answer.

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: D

100% is D

upvoted 1 times

Eltooth 2 years, 3 months ago

Selected Answer: D

D is correct answer.

Teams baby!

upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: D

correct

upvoted 1 times

shubadadasgaonkar 3 years, 3 months ago

The answer is correct- Teams

upvoted 5 times

Question #18 *Topic 6*

You are developing a multi-tier application. The application will use Azure App Service web apps as the front end and an Azure SQL database as the back end.
The application will use Azure functions to write some data to Azure Storage.
You need to send the Azure DevOps team an email message when the front end fails to return a status code of 200.
Which feature should you use?

A. Service Map in Azure Log Analytics

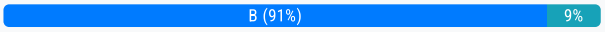
B. availability tests in Azure Application Insights

C. Profiler in Azure Application Insights

D. Application Map in Azure Application Insights

Suggested Answer: *D*
Application Map helps you spot performance bottlenecks or failure hotspots across all components of your distributed application. Each node on the map represents an application component or its dependencies; and has health KPI and alerts status.
Incorrect Answers:
A: Service Map automatically discovers application components on Windows and Linux systems and maps the communication between services. You can use it to view your servers as you think of them--interconnected systems that deliver critical services. Service Map shows connections between servers, processes, and ports across any TCP-connected architecture with no configuration required, other than installation of an agent.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-map

Community vote distribution



artisticcheese Highly Voted 4 years, 9 months ago
Correct answer is B
upvoted 120 times

rhr 4 years, 7 months ago
No D is right answer
upvoted 8 times

Abhishek81 4 years, 2 months ago
B is correct.
https://docs.microsoft.com/en-us/azure/azure-monitor/learn/tutorial-alert
upvoted 23 times

silverdeath Highly Voted 4 years, 5 months ago
the correct answer is B,
After you've deployed your web app/website, you can set up recurring tests to monitor availability and responsiveness. Azure Application Insights sends web requests to your application at regular intervals from points around the world. It can "alert" you if your application isn't responding, or if it responds too slowly.
https://docs.microsoft.com/en-us/azure/azure-monitor/app/monitor-web-app-availability
upvoted 24 times

praveen97 4 years, 2 months ago
Yes B is the correct answer.
upvoted 4 times

mrg998 1 year, 8 months ago
just tried it, this is correct
upvoted 1 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: B

B. availability tests in Azure Application Insights
https://learn.microsoft.com/en-us/azure/azure-monitor/app/availability-alerts
upvoted 1 times

vsvaid 9 months ago
Selected Answer: B
B for me
upvoted 1 times

Firdous586 9 months, 3 weeks ago
B is the correct answer:
After you've deployed your web app or web site to any server, you can set up tests to monitor its availability and responsiveness. Application Insights sends web requests to your application at regular intervals from points around the world. It alerts you if your application doesn't respond or responds slowly.

For more information you can follow this Link.
https://azuredevopslabs.com/labs/azuredevops/appinsights/
Note: Microsoft will ask more questions about Devops
upvoted 1 times

zellck 1 year, 3 months ago
Selected Answer: B
B is the answer.

https://learn.microsoft.com/en-us/azure/azure-monitor/app/availability-overview
After you've deployed your web app or website, you can set up recurring tests to monitor availability and responsiveness. Application Insights sends web requests to your application at regular intervals from points around the world. It can alert you if your application isn't responding or responds too slowly.

You can set up availability tests for any HTTP or HTTPS endpoint that's accessible from the public internet. You don't have to make any changes to the website you're testing. In fact, it doesn't even have to be a site that you own. You can test the availability of a REST API that your service depends on.
upvoted 3 times

alexax578 2 years ago
Selected Answer: B
D does not send email alerts
upvoted 2 times

giuliohome 2 years ago
Selected Answer: B
Changed my ming, even though D - application map - is more sophisticated there is no obvious way to create a direct alert with (email notification) from there while availability tests can directly create alerts, so I imagine one should only test GET read API in Production... In that case I agree that the answer is B.
upvoted 3 times

giuliohome 2 years ago
Selected Answer: D
It must be D and not B. Imagine it is Production and you cannot call a backend service that would trigger changes in Production. You have to monitor what happens in Production, you can't touch and change the data as in a test environment, you only want to map user-calls and discover user-side, frontend problems. Answer B would be valid only for test environments and that is not specified in the question, instead all let us think it could well be an app in Production.
upvoted 1 times

gabo 11 months, 3 weeks ago
Availability Test doesn't modify any data, you can even use it to monitor some external site/service. So that's definitely the answer.
upvoted 2 times

syu31svc 2 years, 1 month ago
Selected Answer: B
https://docs.microsoft.com/en-us/azure/azure-monitor/app/availability-azure-functions

I would take B as the answer

upvoted 2 times

Drummer 2 years, 2 months ago

The correct answer is B

https://docs.microsoft.com/en-us/azure/azure-monitor/app/monitor-web-app-availability

upvoted 2 times

supernovas 2 years, 3 months ago

Selected Answer: B

its correct

upvoted 2 times

R00tsr0ck 2 years, 3 months ago

Selected Answer: D

Application Map with an alert will make more sense, as we need to alert every time the applications fails to send a 200 response code

upvoted 2 times

Eltooth 2 years, 3 months ago

Selected Answer: B

B is correct answer.

upvoted 2 times

UnknowMan 2 years, 4 months ago

Selected Answer: B

B is Correct

upvoted 2 times

Cheehp 2 years, 5 months ago

Selected during exam.

B. availability tests in Azure Application Insights

upvoted 1 times

Whirly 2 years, 5 months ago

Correct Answer is D, very similar question in measureup and the answer is Application mapping.

upvoted 3 times

Question #19 *Topic 6*

You have a project in Azure DevOps named Project1. Project1 contains a published wiki.
You need to change the order of pages in the navigation pane of the published wiki in the Azure DevOps portal.
What should you do?

A. At the root of the wiki, create a file named .order that defines the page hierarchy.

B. At the root of the wiki, create a file named wiki.md that defines the page hierarchy.

C. Rename the pages in the navigation pane.

D. Drag and drop the pages in the navigation pane.

Suggested Answer: *D*
Reorder a wiki page -
You can reorder pages within the wiki tree view to have pages appear in the order and hierarchy you want. You can drag-and-drop a page title in the tree view to do the following operations:
➪ Change the parent-child relationship of a page
➪ Change the order of the page within the hierarchy
Reference:
https://docs.microsoft.com/en-us/azure/devops/project/wiki/add-edit-wiki

Community vote distribution
A (70%) D (30%)

franekfranek Highly Voted 2 years, 3 months ago
Selected Answer: A
"To structure the list of pages in the navigation pane for a *publish code as wiki*, define the .order file at the root, and for each subfolder or parent page that contains subpages."
"The *provisioned* wiki manages the page sequence and page list automatically as you add or move pages within the navigation pane."

https://docs.microsoft.com/en-us/azure/devops/project/wiki/provisioned-vs-published-wiki?view=azure-devops#page-sequence-and-page-list-in-navigation-pane
upvoted 22 times

SenseiJC 1 year ago
This is specific to a provisioned wiki or "code as wiki" but the question is more general. So answer D is better.
upvoted 2 times

Smartiup 11 months ago
"Project1 contains a *published* wiki." Published means wiki as code in a markdown .md file. Editing the .order file is the the correct and only answer.
upvoted 2 times

syu31svc Highly Voted 2 years, 1 month ago
Selected Answer: A
https://docs.microsoft.com/en-us/azure/devops/project/wiki/wiki-file-structure?view=azure-devops#order-file

"The .order file defines the sequence of pages within the wiki."

Answer is A
upvoted 11 times

AnishGS Most Recent 6 months, 1 week ago
A
Tested in my account
upvoted 1 times

AnishGS 6 months, 1 week ago
Sorry. The option is D.
Answer A is a typo

upvoted 1 times

Shachar_Nativ 6 months, 4 weeks ago

Selected Answer: D

"You can reorder pages within the wiki tree view to have pages appear in the order and hierarchy you want. You can drag-and-drop a page title in the tree view to do the following operations:

* Change the parent-child relationship of a page.
* Change the order of the page within the hierarchy.
"

https://learn.microsoft.com/en-us/azure/devops/project/wiki/add-edit-wiki?view=azure-devops&tabs=browser#reorder-a-wiki-page

upvoted 2 times

Munwalinwali 7 months, 3 weeks ago

Answer is A.
https://learn.microsoft.com/en-us/azure/devops/project/wiki/wiki-file-structure?view=azure-devops#order-file

upvoted 1 times

ServerBrain 8 months, 2 weeks ago

Selected Answer: D

Questions says 'change the order of pages in the navigation pane' so why not simply
Drag and drop the pages in the navigation pane???

upvoted 1 times

MeysamBayani 9 months, 2 weeks ago

You can reorder pages within the wiki tree view to have pages appear in the order and hierarchy you want. You can drag-and-drop a page title in the tree view to do the following operations:

Change the parent-child relationship of a page.
Change the order of the page within the hierarchy.

upvoted 1 times

Firdous586 10 months, 2 weeks ago

D is the answer for this question

Already tested this in lab you can simply drag and drop

upvoted 1 times

Firdous586 9 months, 3 weeks ago

After checking with MS Documents:
I am changing my earlier answer
A is the correct option for Published Wiki but for other option you can drag and drop
This is because if you try to drag and drop in Published Wiki your links may get break and you have to manually need to change it therefore you need to change it from Root Directory it self to make order

upvoted 2 times

yana_b 1 year ago

Selected Answer: D

D is the option to reorder it in the Navigation pane (drag & drop on the nav. pane itself).

.order is a type of file which we create and in this file we specify the desired sequence, but this is not done on the navigation pane

Evidenced by the lab itself:

https://azuredevopslabs.com/labs/azuredevops/wiki/

upvoted 1 times

SenseiJC 1 year ago

Selected Answer: D

Answer D is most appropriate based on the phrasing of the question.
https://learn.microsoft.com/en-us/azure/devops/project/wiki/add-edit-wiki?view=azure-devops&tabs=browser#reorder-a-wiki-page

upvoted 1 times

renzoku 1 year, 2 months ago

Selected Answer: D

Drag and drop

https://learn.microsoft.com/en-us/azure/devops/project/wiki/add-edit-wiki?view=azure-devops&tabs=browser

upvoted 2 times

renzoku 1 year, 1 month ago

Im sorry, I was wrong, the link provided refer to provisioned wiki, not published wiki.

The answer should be A.

A. At the root of the wiki, create a file named .order that defines the page hierarchy.

This file allows you to control the page sequence and hierarchy in the navigation pane.

Drag and drop the pages in the navigation pane, available for Provisioned Wikis, for Published Wikis, this option is not available.

https://learn.microsoft.com/en-us/azure/devops/project/wiki/provisioned-vs-published-wiki?view=azure-devops#page-sequence-and-page-list-in-navigation-pane

upvoted 3 times

mcabrito 6 months, 2 weeks ago

You are correct! Nice observation. I would have chosen option D as well, but after your comment, I went to check the documentation from the link you provided, and it does make sense. The correct option for this question is A, precisely because the beginning of the question refers to a "published wiki" and not a "provisioned wiki." Thank you very much.

upvoted 1 times

Pamban 1 year, 2 months ago

Selected Answer: A

It is clear that answer is A

Source: https://learn.microsoft.com/en-us/azure/devops/project/wiki/wiki-file-structure?view=azure-devops#order-file

upvoted 1 times

zellck 1 year, 3 months ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/devops/project/wiki/wiki-file-structure?view=azure-devops#order-file

The .order file defines the sequence of pages within the wiki.

upvoted 2 times

resser 1 year, 5 months ago

Selected Answer: D

Option A is incorrect. We have published wiki, which means that .order file already exists. I am going to choose option D.

upvoted 4 times

Fal991l 1 year, 5 months ago

Selected Answer: D

GPT: To change the order of pages in the navigation pane of a published wiki in the Azure DevOps portal, you should drag and drop the pages in the navigation pane. This is the correct answer.

While you can define the order of pages in a wiki using a .order file at the root of the wiki, this only works for provisioned wikis, not published wikis. A published wiki is backed by a Git repository, so the order of pages is determined by the order of files in the repository.

Renaming pages in the navigation pane will not change their order, and creating a wiki.md file at the root of the wiki will not change the page hierarchy.

Therefore, the best approach to change the order of pages in the navigation pane of a published wiki in the Azure DevOps portal is to simply drag and drop the pages to the desired order.

upvoted 3 times

Fal991l 1 year, 5 months ago

For the question "You need to change the order of pages in the navigation pane of the published wiki in the Azure DevOps portal. What should you do?" the correct answer is actually D. Drag and drop the pages in the navigation pane.

According to Microsoft documentation, you can change the order of pages in the navigation pane by dragging and dropping them into the desired order. The order will be saved automatically. There is no need to create a file such as .order or wiki.md to specify the page hierarchy.

upvoted 2 times

Mc92001 1 year, 8 months ago

asked in my yesterdays exam

upvoted 2 times

elequiel 1 year, 9 months ago

Selected Answer: A

To reorder definitively an .order file is better, because anyone gonna reordering via portal did`nt changing

upvoted 2 times

Question #20 *Topic 6*

DRAG DROP -

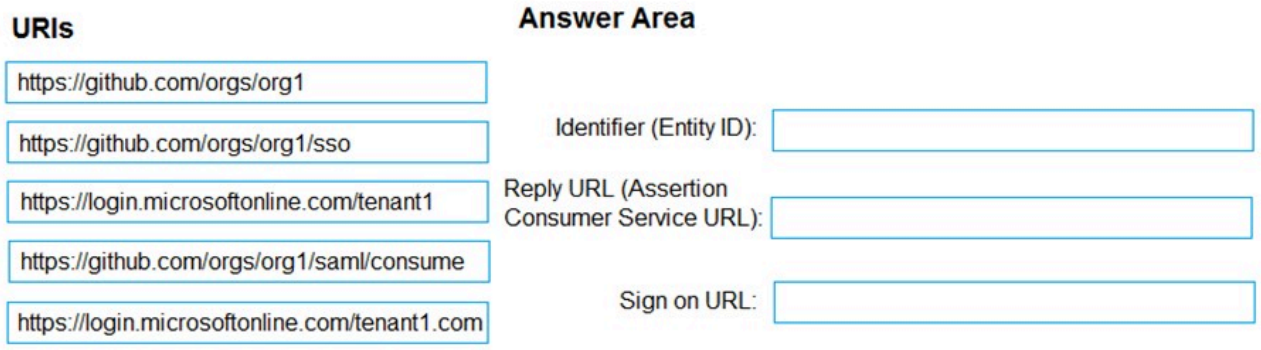
You have a GitHub organization named org1 and an Azure tenant named Tenant1.

You need to enable single sign-on (SSO) in Azure Active Directory (Azure AD) for the users in org1.

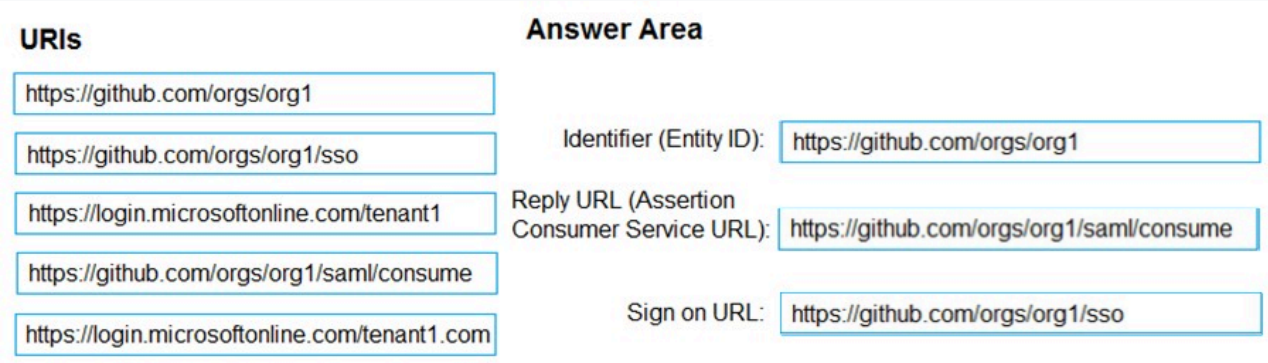
Which URIs should you use for the SAML configuration in Azure AD? To answer, drag the appropriate URIs to the correct settings. Each URI may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested Answer:



Reference:

https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/github-tutorial

vvkds Highly Voted 2 years, 4 months ago

On the Basic SAML Configuration section, enter the values for the following fields:

a. In the Identifier (Entity ID) text box, type a URL using the following pattern: https://github.com/orgs/<Organization ID>

b. In the Reply URL text box, type a URL using the following pattern: https://github.com/orgs/<Organization ID>/saml/consume

c. In the Sign on URL text box, type a URL using the following pattern: https://github.com/orgs/<Organization ID>/sso

upvoted 21 times

mrg998 1 year, 8 months ago

looks right

upvoted 1 times

Akc0 1 year, 4 months ago

But it's also a silly question because anyone who's set up SAML in production knows that the azure page tells you exactly which URLs to grab and paste, there's no need to remember them like this!

upvoted 3 times

SoftwareEngineeringMaster 2 years, 3 months ago

Do not crate your own answers

upvoted 5 times

warchoon 1 year, 9 months ago

https://learn.microsoft.com/en-us/azure/active-directory/saas-apps/github-tutorial

upvoted 3 times

zellck Highly Voted 1 year, 3 months ago

1. https://github.com/orgs/<Organization ID>
2. https://github.com/orgs/<Organization ID>/saml/consume
3. https://github.com/orgs/<Organization ID>/sso

https://learn.microsoft.com/en-us/azure/active-directory/saas-apps/github-tutorial#configure-azure-ad-sso
On the Basic SAML Configuration section, enter the values for the following fields:
a. In the Identifier (Entity ID) text box, type a URL using the following pattern: https://github.com/orgs/<Organization ID>
b. In the Reply URL text box, type a URL using the following pattern: https://github.com/orgs/<Organization ID>/saml/consume
c. In the Sign on URL text box, type a URL using the following pattern: https://github.com/orgs/<Organization ID>/sso
upvoted 9 times

ozbonny Most Recent 6 months, 3 weeks ago
Correct
upvoted 1 times

oiyien_007 1 year ago
https://learn.microsoft.com/en-us/azure/active-directory/saas-apps/github-tutorial
upvoted 1 times

syu31svc 2 years, 1 month ago
Given answer is correct and link supports it
upvoted 5 times

abramq 1 year, 7 months ago
"Given answer"... But given by who? By examtopics OR by vvds user?!
upvoted 2 times

UnknowMan 2 years, 4 months ago
Correct
upvoted 3 times

U3 2 years, 4 months ago
Given answer is correct!
upvoted 3 times

Question #21 *Topic 6*

Your company plans to use an agile approach to software development.
You need to recommend an application to provide communication between members of the development team who work in locations around the world. The applications must meet the following requirements:
➪ Provide the ability to isolate the members of different project teams into separate communication channels and to keep a history of the chats within those channels.
➪ Be available on Windows 10, Mac OS, iOS, and Android operating systems.
➪ Provide the ability to add external contractors and suppliers to projects.
➪ Integrate directly with Azure DevOps.
What should you recommend?

A. Skype for Business

B. Bamboo

C. Octopus

D. Slack

Suggested Answer: *D*
Slack is a popular team collaboration service that helps teams be more productive by keeping all communications in one place and easily searchable from virtually anywhere. All your messages, your files, and everything from Twitter, Dropbox, Google Docs, Azure DevOps, and more all together. Slack also has fully native apps for iOS and Android to give you the full functionality of Slack wherever you go.

Integrated with Azure DevOps -
This integration keeps your team informed of activity happening in its Azure DevOps projects. With this integration, code check-ins, pull requests, work item updates, and build events show up directly in your team's Slack channel.
Note: Microsoft Teams would also be a correct answer, but it is not an option here.
Reference:
https://marketplace.visualstudio.com/items?itemName=ms-vsts.vss-services-slack

Community vote distribution
D (100%)

AS007 Highly Voted 4 years, 4 months ago
Verified - its correct
upvoted 26 times

wpinfo Highly Voted 4 years, 3 months ago
To provide communication between team members, Team is preferred, if there is no Team option, then Slack.
upvoted 19 times

zhshwx Most Recent 5 months ago
I feel that this question might be outdated, as MS Teams has replaced Skype for Business.
upvoted 1 times

Jawad1462 1 year, 10 months ago
Selected Answer: D
Slack is " Team "
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: D
https://marketplace.visualstudio.com/items?itemName=ms-vsts.vss-services-slack

Answer is D
upvoted 1 times

Eltooth 2 years, 3 months ago
Selected Answer: D

D is correct answer.
Slack
upvoted 1 times

UnknowMan 2 years, 4 months ago
Selected Answer: D
Correct, slack is a build in "feature" on az devops
upvoted 1 times

ougullamaija 2 years, 5 months ago
Selected Answer: D
This is true, since Slack and Microsoft seem to be really good friends with each other.
upvoted 3 times

rdemontis 2 years, 5 months ago
Selected Answer: D
correct slack
upvoted 1 times

Aniruddha_dravyakar 2 years, 11 months ago
Slack is correct
upvoted 2 times

amsun10 2 years, 11 months ago
is it an Ad? lol
upvoted 6 times

Jkmr622 3 years, 8 months ago
Slack es correctamundo
upvoted 3 times

gmoorthy 3 years, 8 months ago
answer is correct
upvoted 2 times

kumardeb 3 years, 10 months ago
D. Slack
upvoted 2 times

BabaRamdev 3 years, 10 months ago
I would have gone with Teams followed by Slack. But as Teams not one of the options, will go with Slack. Correct answer.
upvoted 3 times

goku02 4 years, 3 months ago
answer is correct.
upvoted 5 times

webforce08 4 years, 9 months ago
Bamboo: Tie automated builds, tests, and releases together in a single workflow.
upvoted 1 times

bombjack70 4 years, 8 months ago
the topic is about communication so in my opinion the right choice are slack and teams
upvoted 22 times

Question #22 *Topic 6*

You are designing a YAML template for use with Azure Pipelines. The template will include the outputfile parameter.
Which two methods can you use to reference the parameter? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. ${{parameters.outputfile}}

B. $(parameters['outputfile'])

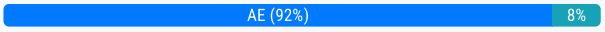
C. $(parameters.outputfile)

D. $(parameters[outputfile])

E. ${{parameters['outputfile']}}

Suggested Answer: *AE*
The parameters section in a YAML defines what parameters are available. Parameters are only available at template parsing time. Parameters are expanded just before the pipeline runs so that values surrounded by ${{ }} are replaced with parameter values.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/process/runtime-parameters

Community vote distribution



pdk88 Highly Voted 1 year, 12 months ago

Selected Answer: AE

${{ parameters['solution'] }} # index syntax
${{ parameters.solution }} # property dereference syntax

https://learn.microsoft.com/en-us/azure/devops/pipelines/process/templates?view=azure-devops#template-expressions
upvoted 11 times

Miten94 Most Recent 2 months, 3 weeks ago

Came in Exam June 23, 2024
upvoted 1 times

ozbonny 6 months, 3 weeks ago

Selected Answer: AE

To reference the outputfile parameter in a YAML template for Azure Pipelines, you can use the ${{ parameters.outputfile }} syntax or the ${{ parameters['outputfile'] }} syntax. Both of these methods are valid and commonly used.

So, the correct options are:

A. ${{parameters.outputfile}}
E. ${{parameters['outputfile']}}
upvoted 1 times

vsvaid 9 months ago

Selected Answer: AE

Agree with answer
upvoted 1 times

zellck 1 year, 3 months ago

Selected Answer: AE

AE is the answer.

https://learn.microsoft.com/en-us/azure/devops/pipelines/process/runtime-parameters?view=azure-devops&tabs=script
Parameters are only available at template parsing time. Parameters are expanded just before the pipeline runs so that values surrounded by ${{ }} are replaced with parameter values. Use variables if you need your values to be more widely available during your pipeline run.
upvoted 4 times

AlexeyG 1 year, 6 months ago
got this in 02 March 2023 exams. scored 870 marks.
upvoted 4 times

lugia4000 1 year, 7 months ago
double curly brackets double curly brackets is the correct
upvoted 2 times

Darkeh 1 year, 12 months ago
Selected Answer: AE
Mohammad is correct - read his comment.
upvoted 3 times

sieira 2 years ago
AE
https://docs.microsoft.com/en-us/azure/devops/pipelines/process/templates?view=azure-devops#template-expressions
upvoted 3 times

MohmmadFayez 2 years ago
Selected Answer: AE
Answer correct
A & B

Parameters can be referenced with Template expressions.
Template Expression there is 2 forms of syntax :

${{ parameters['solution'] }} # index syntax

&
${{ parameters.solution }} # property dereference syntax

https://docs.microsoft.com/en-us/azure/devops/pipelines/process/templates?view=azure-devops#template-expressions

Regarding to C : this is Macro syntax and can be used to reference variables at runtime cant use it with parameters

https://docs.microsoft.com/en-us/azure/devops/pipelines/process/variables?view=azure-devops&tabs=yaml%2Cbatch#runtime-expression-syntax
upvoted 4 times

hebertpena88 2 years ago
Selected Answer: AC
I always use ${{parameters.foo}} and sometimes maybe you will use it with IF then you can use:
${{ if eq(length(parameters.foo), 0) }}:

Thus, only A and C fit in.
upvoted 1 times

syu31svc 2 years ago
Selected Answer: AC
From what is seen from the link, I would take A and C
upvoted 1 times

KozaL 2 years ago
Should be A,C
upvoted 1 times

Question #1 *Topic 7*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You need to recommend an integration strategy for the build process of a Java application. The solution must meet the following requirements:

- The build must access an on-premises dependency management system.
- The build outputs must be stored as Server artifacts in Azure DevOps.
- The source code must be stored in a Git repository in Azure DevOps.

Solution: Configure the build pipeline to use a Microsoft-hosted agent pool running the Windows Server 2019 with Visual Studio 2019 image. Include the Java Tool

Installer task in the build pipeline.

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*

To build and deploy Windows, Azure, and other Visual Studio solutions you'll need at least one Windows agent. Windows agents can also build Java and Android apps.

The Azure Pipelines agent pool offers several virtual machine images to choose from, each including a broad range of tools and software. One such image is

Windows Server 2019 with Visual Studio 2019.

Reference:

https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/v2-windows?view=azure-devops https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/hosted?view=azure-devops&tabs=yaml

Community vote distribution

B (100%)

hebertpena88 Highly Voted 2 years ago

We need a self host agent, Microsoft's agents can not access to On-premise resources.

upvoted 21 times

mrg998 1 year, 8 months ago

correct answer is a no because the self hosted agent wont have access to LAN

upvoted 2 times

gabo 11 months, 3 weeks ago

Nor can they retain artifacts, so the answer is NO

upvoted 1 times

liuliangzhou Highly Voted 2 years ago

Selected Answer: B

We need self-hosted agent

https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/agents?view=azure-devops&tabs=browser

upvoted 8 times

jmglezgz Most Recent 5 months ago

Selected Answer: B

We need a self host agent

upvoted 1 times

jmglezgz 5 months ago

Selected Answer: B

We need a self host agent

upvoted 1 times

chloaus 5 months ago

See explanation in this link: https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/agents?view=azure-devops&tabs=yaml%2Cbrowser#install

upvoted 1 times

ozbonny 6 months, 3 weeks ago

Selected Answer: B

No -> for on-premises is self-hosted

upvoted 1 times

vsvaid 8 months, 4 weeks ago

Selected Answer: B

Need self hosted

upvoted 1 times

Firdous586 10 months, 3 weeks ago

B is required for onpremise

upvoted 1 times

kleetuss14 11 months ago

Selected Answer: B

Answer is B. You need self hosted agent to support the on-premise requirement.

upvoted 1 times

Pamban 1 year, 2 months ago

this series of yes/no question appeared on today's (20/06/23) exam. the given answer in examtopics seems not correct. Correct answer is to get self host agent and Microsoft's agents has nothing todo with On-premise resources

scored 955. should be correct! cheers

upvoted 2 times

elequiel 1 year, 9 months ago

Selected Answer: B

Need a self hoste agent

upvoted 1 times

Jawad1462 1 year, 10 months ago

Selected Answer: B

Correct

upvoted 2 times

Darkeh 1 year, 12 months ago

Selected Answer: B

B is the correct answer

upvoted 6 times

Question #2 *Topic 7*

You have a project in Azure DevOps.
You create the following YAML template named Template1.yml.
steps:
- script: npm install
- script: yarn install
- script: npm run compile
You create the following pipeline named File1.yml.
parameters:
usersteps:
- task: MyTask@1
- script: echo Done
You need to ensure that Template1.yaml runs before File1.yml.
How should you update File1.yml?

A. parameters: usersteps: extends: template: template1.yml - task: MyTask@1 - script: echo Done

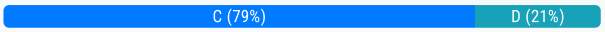
B. template: template1.yml parameters: usersteps: - task: MyTask@1 - script: echo Done

C. extends: template: templatel.yml parameters: usersteps: - task: MyTask@1 - script: echo Done

D. parameters: usersteps: - template: templatel.yml - task: MyTask@1 - script: echo Done

Suggested Answer: *C*
Azure Pipelines offers two kinds of templates: includes and extends. Included templates behave like #include in C++: it's as if you paste the template's code right into the outer file, which references it. To continue the C++ metaphor, extends templates are more like inheritance: the template provides the outer structure of the pipeline and a set of places where the template consumer can make targeted alterations.
Example:
extends:
template: template.yml@templates
parameters:
usersteps:
- script: echo This is my first step
- script: echo This is my second step
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/security/templates

Community vote distribution



jay158 Highly Voted 2 years, 4 months ago
Selected Answer: C
https://docs.microsoft.com/en-us/azure/devops/pipelines/process/templates?view=azure-devops#extend-from-a-template
upvoted 14 times

adityagoel26 Highly Voted 1 year, 5 months ago
Answer should be B. template: template1.yml

Explanation: To ensure that the Template1.yaml runs before File1.yml, you can use the template keyword in File1.yml to reference Template1.yaml. The parameters section is used to pass values to the referenced template. In this case, we need to pass the usersteps parameter from File1.yml to Template1.yaml. Therefore, we need to include the parameters section in File1.yml, and reference the usersteps parameter in Template1.yaml. The correct syntax is shown in option B.

https://learn.microsoft.com/en-us/azure/devops/pipelines/process/templates?view=azure-devops#step-reuse
upvoted 8 times

vsvaid Most Recent 8 months, 4 weeks ago
Cannot figure out how C will work. Looked at the links as well. Not sure which one is answer.
upvoted 1 times

gabo 11 months, 3 weeks ago

Selected Answer: D

As per https://learn.microsoft.com/en-us/azure/devops/pipelines/process/templates?view=azure-devops&pivots=templates-includes#extend-from-a-template

D is a correct option to run the template1.yml code before the steps of File1.yml

upvoted 4 times

gabo 11 months, 3 weeks ago

For those choosing option B, pls note that the syntax is wrong although your thinking of include is correct. The correct syntax in that case should be

parameters: steps: - template: template1.yml - task: MyTask@1 - script: echo Done

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: C

https://docs.microsoft.com/en-us/azure/devops/pipelines/process/templates?view=azure-devops

Answer is C

upvoted 1 times

Sunny1710 2 years, 3 months ago

Correct

upvoted 3 times

Question #3 *Topic 7*

You have an Azure solution that contains a build pipeline in Azure Pipelines.
You experience intermittent delays before the build pipeline starts.
You need to reduce the time it takes to start the build pipeline.
What should you do?

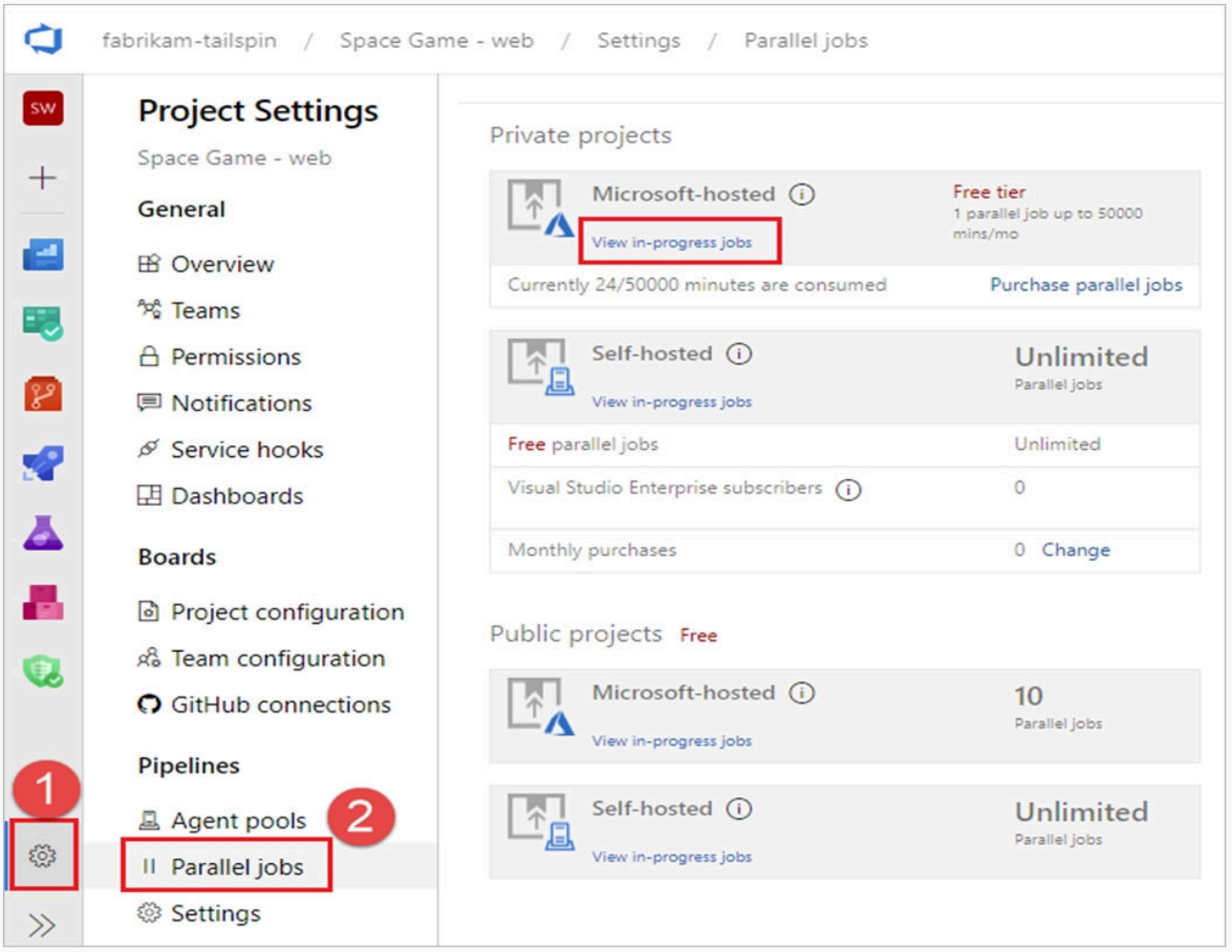
A. Enable self-hosted build agents.

B. Create a new agent pool.

C. Split the build pipeline into multiple stages.

D. Purchase an additional parallel job.

Suggested Answer: *D*
We need to ensure that resources are available without a startup delay. We don't have enough concurrency.
To check how much concurrency you have:
To check your limits, navigate to Project settings, Parallel jobs.



Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/troubleshooting/troubleshooting

Community vote distribution
D (51%) A (49%)

alpars Highly Voted 2 years, 3 months ago
build delays are related wit concurrence! self hosted vs windows hosted does not affect the delays. Hence, I believe given answer is correct. It is D.
upvoted 31 times

jose Highly Voted 1 year, 9 months ago
Selected Answer: A

"You experience intermittent delays before the build pipeline starts."
Before starts... So (A) "Enable self-hosted build agents" reduce the time it taks to start the build pipeline.
Purchase and additional parallel job could help to reduce the execution time of the build pipeline, not the delay to start, because the build pipeline has to wait for a free agent to start
upvoted 15 times

gerardjongh 5 months ago
Not entirely true because when a job is already running a new job has to wait for the other one to finish before it starts.....
upvoted 2 times

DevopsRock Most Recent 1 week ago
Selected Answer: D
D. Purchase an additional parallel job. You have to wait for an agent to pick up the task no matter what.
upvoted 1 times

sondrex 1 month, 3 weeks ago
D. Purchase an additional parallel job.
upvoted 1 times

GPRai 2 months, 3 weeks ago
Selected Answer: A
I will Choose A, due to start timing of the build job
upvoted 1 times

FeriAZ 5 months, 3 weeks ago
Selected Answer: D
In this specific scenario where delays occur before the pipeline even starts, the issue lies in the availability of a free agent to handle the build job. Purchasing an additional parallel job increases the number of concurrent pipelines that can be executed on the same agent, potentially reducing the queueing time for your pipeline to find an available agent.
upvoted 5 times

ozbonny 6 months, 3 weeks ago
Selected Answer: A
Correct A

If you are just setting up a pipeline and are comparing the performance of Microsoft-hosted agents to your local machine or a self-hosted agent, then note the specifications of the hardware that we use to run your jobs. We are unable to provide you with bigger or powerful machines. You can consider using self-hosted agents or scale set agents if this performance is not acceptable.

https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/hosted?view=azure-devops&tabs=yaml
upvoted 2 times

Munwalinwali 7 months, 3 weeks ago
Selected Answer: A
After reading all comments, I went with A
upvoted 1 times

hardinxcore 8 months, 3 weeks ago
Selected Answer: A
I'd choose A. While D would be a valid answer if the the delay would be caused by another job running, that aspect is not mentioned in the question at all.
upvoted 1 times

vsvaid 8 months, 4 weeks ago
Selected Answer: D
Purchase an additional parallel job will help
upvoted 2 times

mfawew223 10 months ago
Selected Answer: D
I think the answer is D. The word "intermittent" in the question implies irregular interval delays. While switching from MS-hosted to self-hosted would improve the startup time, that improvement comes from the fact that MS-hosted has to boot fresh every time but a self-hosted agent doesnt because it stays alive for you, caches, etc

MS-hosted build agents loading would not be described as intermittent, because the spin-up time would be about the same each iteration, given similar/identical pipelines.

What WOULD be intermittent is having to wait for other pipeline's jobs to finish before yours starts, and that is an irregular interval (i.e. intermittent) being created

upvoted 5 times

cluqueg 10 months, 3 weeks ago

Selected Answer: D

D is correct and probably is intended to be the target answer.

upvoted 2 times

yana_b 10 months, 4 weeks ago

Here are few ways you can achieve faster builds:

- Choosing agents that meet your performance requirements
- Build server location
- Scaling out build servers
- Optimizing the build: Add parallel jobs to speed up the build process

https://learn.microsoft.com/en-us/azure/well-architected/devops/release-engineering-performance

upvoted 1 times

gabo 11 months, 3 weeks ago

This is a tricky question because:

If delay is due to agent busy : Answer will be Increase Parallel processes

If delay is due to agent not ready : Answer will be choose a Self Hosted Agent that would startup quickly

upvoted 5 times

xRiot007 1 year, 1 month ago

A - self hosted agents.

In a pipeline jobs can also be forced to run sequently for different reason. Puschasing more agents will not solve this issue.

A self hosted agent will start faster than one from the pool. Always.

Intermitent delays might also be cause because all agents are queued.

A self hosted agent also solves this because it will be at your disposal, so each time YOU trigger a build it will be immediately available for you.

upvoted 2 times

tomhansen 1 year, 4 months ago

ChatGPT says its A

upvoted 1 times

kevin9988 1 year, 4 months ago

Selected Answer: D

It should be D

upvoted 3 times

Question #4 *Topic 7*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You need to recommend an integration strategy for the build process of a Java application. The solution must meet the following requirements:

- ➪ The build must access an on-premises dependency management system.
- ➪ The build outputs must be stored as Server artifacts in Azure DevOps.
- ➪ The source code must be stored in a Git repository in Azure DevOps.

Solution: Configure the build pipeline to use a Microsoft-hosted agent pool running a Linux image. Include the Java Tool Installer task in the build pipeline.

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*

To run your jobs, you'll need at least one agent. A Linux agent can build and deploy different kinds of apps, including Java and Android apps.

If your pipelines are in Azure Pipelines and a Microsoft-hosted agent meets your needs, you can skip setting up a private Linux agent.

The Azure Pipelines agent pool offers several virtual machine images to choose from, each including a broad range of tools and software.

We support Ubuntu,

Red Hat, and CentOS.

Reference:

https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/v2-linux?view=azure-devops https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/hosted?view=azure-devops&tabs=yaml

Community vote distribution

B (95%) 5%

UnknowMan Highly Voted 2 years, 4 months ago

Selected Answer: B

Microsoft agent != on-prem

upvoted 13 times

megleg Most Recent 1 week, 4 days ago

Self hosted hands the on prem part

upvoted 1 times

vsvaid 8 months, 4 weeks ago

Selected Answer: B

Self hosted is required to access on-premesis

upvoted 1 times

gabo 11 months, 3 weeks ago

Selected Answer: B

Microsoft Agent will not retain artifacts

upvoted 1 times

yana_b 1 year, 1 month ago

Selected Answer: B

When we speak about on-prem => self-hosted agent, as MS hosted agents are not relevant for on-premises

upvoted 2 times

mrg998 1 year, 8 months ago

Selected Answer: B

answer is no, needs to get to on-repm
upvoted 2 times

elequiel 1 year, 9 months ago

Selected Answer: B

Answer is No

Onpremisse depedency
upvoted 2 times

SerdarG 2 years, 1 month ago

Selected Answer: B

You cannot use Microsoft-hosted agents or the Azure Pipelines agent pool with on-premises TFS or Azure DevOps Server.
https://docs.microsoft.com/bs-latn-ba/azure/devops/pipelines/agents/hosted?view=azure-devops-2020&tabs=yaml
upvoted 4 times

syu31svc 2 years, 1 month ago

Selected Answer: B

on-premises so self-hosted

Answer is No
upvoted 1 times

prasad2222 2 years, 1 month ago

Answer is A
upvoted 1 times

basw77 2 years, 2 months ago

Selected Answer: B

Access to on-prem system, so always self-hosted agent
upvoted 4 times

YUCHAN2022 2 years, 4 months ago

Selected Answer: A

Must be A
upvoted 2 times

dstux 2 years, 4 months ago

Selected Answer: B

Microsoft agent will not have access to on-prem libs
upvoted 2 times

demonite 2 years, 4 months ago

But you can configure it to have access to on-prem, Ans A
upvoted 1 times

thiagotteles 2 years, 4 months ago

but not describet in solution... Correct is B
upvoted 1 times

xRiot007 1 year, 1 month ago

It can be, but it's not set here, so answer is B
upvoted 1 times

Dave43 2 years, 4 months ago

Selected Answer: B

Anseer is B
upvoted 4 times

Question #5 *Topic 7*

You store source code in a Git repository in Azure Repos. You use a third-party continuous integration (CI) tool to control builds.
What will Azure DevOps use to authenticate with the tool?

A. certificate authentication

B. a personal access token (PAT)

C. a Shared Access Signature (SAS) token

D. NTLM authentication

Suggested Answer: *B*
Personal access tokens (PATs) give you access to Azure DevOps and Team Foundation Server (TFS), without using your username and password directly.
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/git/auth-overview

Community vote distribution
B (100%)

27close Highly Voted 3 years, 10 months ago
PAT- answer
upvoted 17 times

igorole Highly Voted 3 years, 2 months ago
The question says:
What will Azure DevOps use to authenticate with the tool?

Azure devops will not use anything. The third party CI tool will use a PAT to access l Azure DevOps repos.
upvoted 8 times

Akc0 1 year, 4 months ago
Authentication is a 2 way street, PAT will be authenticated between azure devops and the 3rd party CI. The question could have been framed slightly better but still correct
upvoted 1 times

yana_b Most Recent 1 year, 1 month ago
Either PAT or SSH, since there is no SSH amongst the answers => PAT.
upvoted 1 times

renzoku 1 year, 1 month ago
Selected Answer: B
B. a personal access token (PAT)
PATs are short-lived, limited-privilege tokens.
Provided by Azure DevOps, can be used to authenticate/authorize API requests to Azure DevOps services.
Do not share your username and password.

Shared Access Signature (SAS) token, grant access to Azure resources, such as Azure Storage, Azure Service Bus, blob and files. Would be less secure, because SAS tokens are not time-limited and they can grant access to all of your Azure DevOps resources
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: B
100% is B
upvoted 2 times

Eltooth 2 years, 4 months ago
Selected Answer: B
B is correct answer.

upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: B

correct

upvoted 1 times

Gogu83 2 years, 9 months ago

Selected Answer: B

B is correct

upvoted 2 times

poplovic 3 years, 1 month ago

PAT is correct.

either PAT or SSH. https://docs.microsoft.com/en-us/azure/devops/repos/git/auth-overview?view=azure-devops

upvoted 3 times

kumardeb 3 years, 10 months ago

B. a personal access token (PAT)

upvoted 7 times

27close 3 years, 10 months ago

you can authenticate through browser (user name and password) or via API. The APs has 3 options - PAT, web application flows and GitHub App. Given the answers that listed, the right answer should be pAT

upvoted 3 times

DRAG DROP -

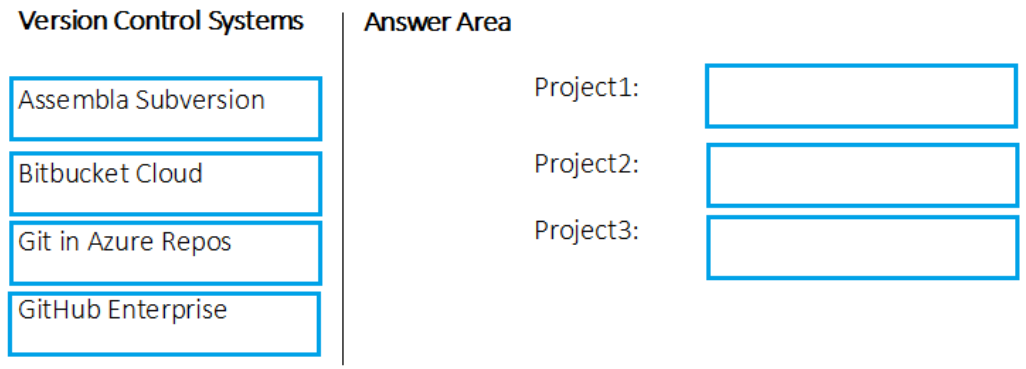
You are configuring Azure Pipelines for three projects in Azure DevOps as shown in the following table.

Project name	Project Details
Project1	The project team provides preconfigured YAML files that it wants to use to manage future pipeline configuration changes.
Project2	The sensitivity of the project requires that the source code be hosted on the managed Windows server on your company's network.
Project3	The project team requires a centralized version control system to ensure that developers work with the most recent version.

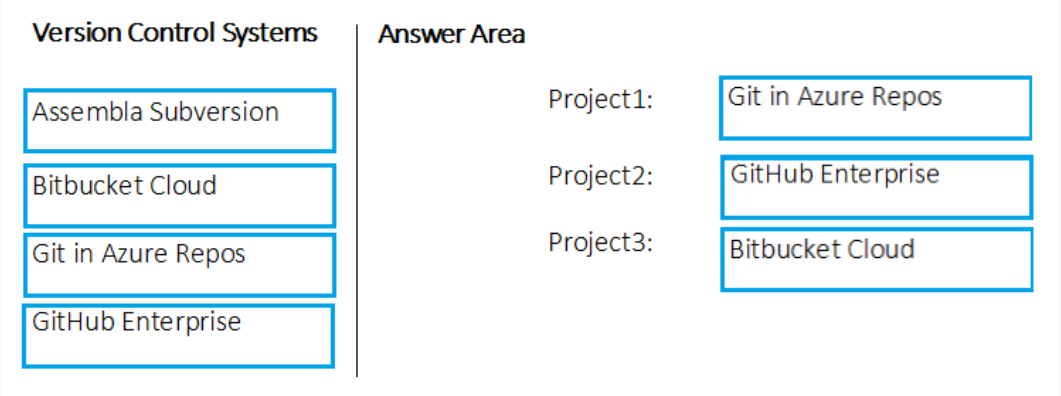
Which version control system should you recommend for each project? To answer, drag the appropriate version control systems to the correct projects. Each version control system may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested Answer:



Project1:Git in Azure Repos -

Project2: Github Enterprise -

GitHub Enterprise is the on-premises version of GitHub.com. GitHub Enterprise includes the same great set of features as GitHub.com but packaged for running on your organization's local network. All repository data is stored on machines that you control, and access is integrated with your organization's authentication system (LDAP, SAML, or CAS).

Project3: Bitbucket cloud -

One downside, however, is that Bitubucket does not include support for SVN but this can be easily amended migrating the SVN repos to Git with tools such as

SVN Mirror for Bitbucket .

Note: SVN is a centralized version control system.

Incorrect Answers:

Bitbucket:

Bitbucket comes as a distributed version control system based on Git.
Note: A source control system, also called a version control system, allows developers to collaborate on code and track changes. Source control is an essential tool for multi-developer projects.
Our systems support two types of source control: Git (distributed) and Team Foundation Version Control (TFVC). TFVC is a centralized, client-server system. In both Git and TFVC, you can check in files and organize files in folders, branches, and repositories.
Reference:
https://www.azuredevopslabs.com/labs/azuredevops/yaml/
https://enterprise.github.com/faq

TosO Highly Voted 4 years, 6 months ago
1 -> Git in Azure DevOps
2 -> Github Enterprise
3 -> Subversion
upvoted 134 times

SoftwareEngineeringMaster 2 years, 3 months ago
%100 wrong answer….. the correct as given above….
You get from where Git in Azure DevOps. Even you %100 right you still need to follow the rule who wrote the test. :)
upvoted 2 times

Dani_ac7 1 year, 2 months ago
3 -> Subversion --> Is subversion because "centralized" = Subersion, "distrubited" = git
upvoted 1 times

MSMaster2020 3 years, 7 months ago
Are we missing an option for Gihub in Azure DevOps in the Version Control Systems?
upvoted 2 times

Samhara Highly Voted 4 years, 3 months ago
Verified
1 -Git in Azure DevOps
2 - Github Enterprise
3 - Subversion
upvoted 27 times

ozbonny Most Recent 6 months, 3 weeks ago
Azure Repos
Github Enterprise
Bitbucket Cloud
upvoted 3 times

vsvaid 8 months, 4 weeks ago
3rd option should be subversion. Subversion (SVN) and TFS are centralized system. Git is distributed
upvoted 1 times

zellck 1 year, 3 months ago
1. Git in Azure repos
2. GitHub Enterprise
3. Subversion

https://learn.microsoft.com/en-us/training/modules/describe-types-of-source-control-systems/2-understand-centralized
ome of the most common-centralized version control systems you may have heard of or used are Team Foundation Version Control (TFVC), CVS, Subversion (or SVN), and Perforce.
upvoted 5 times

zellck 1 year, 3 months ago
https://docs.github.com/en/enterprise-server@3.5/admin/overview/about-github-enterprise-server
GitHub Enterprise Server is a self-hosted platform for software development within your enterprise. Your team can use GitHub Enterprise Server to build and ship software using Git version control, powerful APIs, productivity and collaboration tools, and integrations.

GitHub Enterprise Server runs on your infrastructure and is governed by access and security controls that you define, such as firewalls,

network policies, IAM, monitoring, and VPNs. GitHub Enterprise Server is suitable for use by enterprises that are subject to regulatory compliance, which helps to avoid issues that arise from software development platforms in the public cloud.
upvoted 5 times

Rams_84zO6n 1 year, 6 months ago
1. Git in Azure repos
2. Github Enterprise
3. Subversion
https://www.azuredevopslabs.com/labs/azuredevops/yaml/#task-4-adding-a-yaml-build-definition
When you define a new pipeline and choose a repo from Azure Repos Git, you get the option to pick a pre-configured YAML configuration.
upvoted 1 times

lugia4000 1 year, 7 months ago
Came out at 20230215
upvoted 7 times

syu31svc 2 years, 1 month ago
Project 1 "preconfigured YAML" so Git in Azure Repos
Project 2 "company network so GitHub Enterprise"
Project 3 "centralized version control" so subversion
upvoted 3 times

UnknowMan 2 years, 4 months ago
1 -> Git in Azure DevOps -> CICD
2 -> Github Enterprise -> On Premise GitHub
3 -> Subversion -> Centralized (git is decentralized)
upvoted 4 times

rdemontis 2 years, 5 months ago
IMHO answers are
1. Git in Azure DevOps
2. GitHub Enterprise
3. Subversion

As the answer explanation itself states Bitbucket is decentralized like Git.
upvoted 3 times

lugospod 2 years, 7 months ago
Got this January 2022.
upvoted 3 times

celciuz 3 years ago
This question came out, August 2021.

The correct answer should be:
1. Git in Azure Repos
- You can store YAML pipeline config files in Azure Repos Git to be referenced in your Pipelines.
2. GitHub Enterprise
- Only solution here that enables you to host your Git Repo on premise privately
3. Assembla Subversion
- SVN is a centralized version control.
upvoted 5 times

celciuz 3 years ago
This question came out, August 2021
upvoted 1 times

Ravi22 3 years, 3 months ago
1 Git in Azure Repos
2 Github Enterprise
3 Aseembla Subversion

--Varified answer
upvoted 5 times

Sri_Hari 3 years, 5 months ago

Git in Azure Repos

GitHub Enterprise

Assembla Subversion

upvoted 4 times

RKS 3 years, 7 months ago

1 -> Git in Azure DevOps

2 -> Github Enterprise

3 -> Subversion

upvoted 1 times

vglearn 3 years, 7 months ago

Answer Should be

1-> Git in Azure Repos

2->GitHub Enterprise

3->Subversion

Explanation

1. Here since you are going to making use of YAML files for Azure Pipelines, the best solution would be to use Git in Azure Repos
2. Here you can use GitHub Enterprise. This allows you to host a Git repository on your on-premise environment to keep it private.
3. Subversion is a centralized source code versioning system.

upvoted 7 times

Question #7 *Topic 7*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You need to recommend an integration strategy for the build process of a Java application. The solution must meet the following requirements:

- ➪ The builds must access an on-premises dependency management system.
- ➪ The build outputs must be stored as Server artifacts in Azure DevOps.
- ➪ The source code must be stored in a Git repository in Azure DevOps.

Solution: Configure an Octopus Tentacle on an on-premises machine. Use the Package Application task in the build pipeline.

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*

Octopus Deploy is an automated deployment server that makes it easy to automate deployment of ASP.NET web applications, Java applications, NodeJS application and custom scripts to multiple environments.

Octopus can be installed on various platforms including Windows, Mac and Linux. It can also be integrated with most version control tools including VSTS and

GIT.

When you deploy software to Windows servers, you need to install Tentacle, a lightweight agent service, on your Windows servers so they can communicate with the Octopus server.

When defining your deployment process, the most common step type will be a package step. This step deploys your packaged application onto one or more deployment targets.

When deploying a package you will need to select the machine role that the package will be deployed to.

Reference:

https://octopus.com/docs/deployment-examples/package-deployments https://explore.emtecinc.com/blog/octopus-for-automated-deployment-in-devops-models

Community vote distribution

B (100%)

poplovic Highly Voted 2 years, 12 months ago

Hey guys, this is an exam for Azure, not for Octopus. Do not over-think. The right approach should be and always be around Azure. The key point is the on-premises dependency management system. In Azure, the self-host build agent is designed for this purpose. The self-host agent is in the default agent pool. The rest of requirements could be done in ADO.

So the answer is NO.

upvoted 78 times

GPRai 2 months, 3 weeks ago

Yes, that is correct

upvoted 1 times

UrbanRellik 3 months, 2 weeks ago

Well said.

upvoted 1 times

d0bermannn 2 years, 11 months ago

best comment here

upvoted 7 times

levo017 Highly Voted 4 years, 5 months ago

I think answer is NO, Octopus is a deployment tool, I don't see how it helps with build process.

upvoted 23 times

Praj 3 years, 3 months ago
I Like to move it move it :D
upvoted 3 times

omw2wealth 2 years, 9 months ago
"us" each time we start studying for a certification &deciding the correct answer in examtopics x)
upvoted 1 times

ScreamingHand 3 years, 1 month ago
I remember hearing that track 25 years ago
upvoted 4 times

d0bermannn 3 years ago
imho that was too sleasy, i 'd prefer 1 bourbone, 1 scotch, 1 beer))
upvoted 3 times

Velumani 4 years, 4 months ago
Octobus is the deployment tool only. As per the question we use buld pipeline in azuredevops and get the dependecny packages from octubus server. So the answer is correct I think
upvoted 2 times

kcinofni 4 years, 4 months ago
According to this lab 'https://azuredevopslabs.com/labs/vstsextend/octopus/' Octopus is able to help with the build process, it has appropriate build tasks. For instance, Package Application task can 'package the ASP.NET Core build output into a zip file with the version number'.
upvoted 2 times

Kalaismile06 3 years, 3 months ago
Octopus Deploy is an automated deployment and release management server. It is designed to simplify deployment of ASP.NET applications Windows Services and databases. So, the given answer is correct.
upvoted 1 times

jay158 2 years, 8 months ago
But app here is Java app, not ASP.Net
upvoted 2 times

chloaus Most Recent 5 months ago
B. Octopus Tentacle is a lightweight agent service used for communicating with Octopus server.
https://octopus.com/docs/infrastructure/deployment-targets/tentacle
upvoted 1 times

vsvaid 8 months, 4 weeks ago
Selected Answer: B
What is creating the build? The build process has to be on primesis as it needs to access on premesis dependencies
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: B
"In Azure DevOps"

Answer is No then
upvoted 2 times

warchoon 1 year, 10 months ago
It meets goal. So "Yes".
upvoted 1 times

[Removed] 2 years, 4 months ago
Correct
upvoted 1 times

Franpb90 2 years, 4 months ago
➪ The build outputs must be stored as Server artifacts in Azure DevOps.
upvoted 3 times

vvkds 2 years, 4 months ago

Selected Answer: B

Should use self hosted agent.

upvoted 3 times

warchoon 1 year, 10 months ago

Agent is not a management system.

upvoted 1 times

Divyayuvi 2 years, 5 months ago

https://azuredevopslabs.com/labs/vstsextend/octopus/

Answer - "YES", Kindly check Excercise-3 (Triggering CI-CD) in the above URL

upvoted 2 times

AlexLiourtas 2 years, 5 months ago

Selected Answer: B

answer b no

upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: B

IMHO answer is NO because the question asks for using the Package Application task in the build pipeline. And it's clearly wrong for CI process. this task is the first step to deployment not for build.

https://azuredevopslabs.com/labs/vstsextend/octopus/

upvoted 1 times

warchoon 1 year, 10 months ago

Publish is also a part of build

https://learn.microsoft.com/en-us/azure/devops/pipelines/publish-pipeline-artifact?view=azure-devops&tabs=yaml

upvoted 1 times

Shreyans 2 years, 7 months ago

Selected Answer: B

No is right answer.

upvoted 1 times

totalz 2 years, 10 months ago

How's the solution satisfy the requirement: ✑ The source code must be stored in a Git repository in Azure DevOps.??

upvoted 1 times

sameer2803 3 years, 2 months ago

All the comments about Octopus not helping the build process is valid and logical and the question can interpreted in a lot of ways.... the buzz word in the question is "integration" and we talk about integration when there is 3rd party tool involved. so the answer "yes" should be correct. did anybody saw this question in Exam?

upvoted 1 times

erickim007 3 years, 3 months ago

Why would we use Octopus when DevOps already have build and release pipelines?

Agents can be self hosted under which can be on-prem as well as Azure VM if we established VPN (site to site) which provides on-prem connectivity. Connection to Azure, Artifacts, and so would be much better using built-in feature.

Therefore the answer should 'No'.

upvoted 2 times

Saterial 3 years, 4 months ago

The answer is yes, you can refer to TechieBloke. While I agree the answer is vague, I believe its suppose to reference the full Octopus Deploy tool which it can do all of the listed requirements.

upvoted 2 times

viswanath_ammiraju 3 years, 4 months ago

on premises means self-hosted !! so answer is not correct

upvoted 1 times

Question #8 *Topic 7*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You need to recommend an integration strategy for the build process of a Java application. The solution must meet the following requirements:

➪ The builds must access an on-premises dependency management system.

➪ The build outputs must be stored as Server artifacts in Azure DevOps.

The source code must be stored in a Git repository in Azure DevOps.

▪

Solution: Install and configure a self-hosted build agent on an on-premises machine. Configure the build pipeline to use the Default agent pool. Include the Java

Tool Installer task in the build pipeline.

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Instead use Octopus Tentacle.

Reference:

https://explore.emtecinc.com/blog/octopus-for-automated-deployment-in-devops-models

Community vote distribution

A (96%) 4%

pkg007 Highly Voted 2 years ago

yaaaaaaaaaas finally ..i have experienced in these types of questions where answer is - Yes / NO - and you can not go back - as you can get the clue - right answer i.e. " Yes " is the last questions usually :-)

upvoted 10 times

gabo 11 months, 3 weeks ago

That's true. I just realized it.

upvoted 1 times

ozbonny Most Recent 6 months, 3 weeks ago

Selected Answer: A

Yes yes yes

upvoted 1 times

vsvaid 8 months, 4 weeks ago

Selected Answer: A

Agree, I had to look at the link provided by anhtvux to check if self hosted agents are hosted in Default pools.

https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/pools-queues?source=recommendations&view=azure-devops&tabs=yaml%2Cbrowser#default-agent-pools

upvoted 1 times

gabo 11 months, 3 weeks ago

Selected Answer: A

Answer is Yes, assuming the Default Pool points to the Self Hosted Agent pool.

upvoted 1 times

yana_b 1 year, 1 month ago

Selected Answer: A

Answer is yes

upvoted 1 times

anhtvux 1 year, 7 months ago

Selected Answer: B

It's wrong due to "configure default agent pools"

upvoted 1 times

anhtvux 1 year, 7 months ago

I was thinking Default Agent pool contains Microsoft hosted. But I was wrong, it contains self-hosted - need to register

upvoted 1 times

anhtvux 1 year, 7 months ago

https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/pools-queues?source=recommendations&view=azure-devops&tabs=yaml%2Cbrowser#default-agent-pools

upvoted 1 times

mrg998 1 year, 8 months ago

Selected Answer: A

1000000% yes

upvoted 4 times

syu31svc 2 years, 1 month ago

Selected Answer: A

This is the solution

Answer is Yes

upvoted 2 times

immoral 2 years, 1 month ago

finally, answer is Yes.

upvoted 1 times

mclovin 2 years, 2 months ago

Selected Answer: A

answer is YES

upvoted 1 times

Amrx 2 years, 2 months ago

Why use octopus tentacle when self-hosted agents do the job lol

upvoted 2 times

UnknowMan 2 years, 4 months ago

Selected Answer: A

Correct, self hosted agent do the job

upvoted 2 times

demonite 2 years, 4 months ago

Selected Answer: A

for sure

upvoted 2 times

Loai 2 years, 4 months ago

Selected Answer: A

yes for sure

upvoted 4 times

rbhatia1 2 years, 4 months ago

It must be yes

upvoted 2 times

U3 2 years, 4 months ago

Should be "yes"

upvoted 2 times

waqas 2 years, 4 months ago

Selected Answer: A

Must be yes.

upvoted 4 times

Question #9 *Topic 7*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You need to recommend an integration strategy for the build process of a Java application. The solution must meet the following requirements:

- ➪ The builds must access an on-premises dependency management system.
- ➪ The build outputs must be stored as Server artifacts in Azure DevOps.
- ➪ The source code must be stored in a Git repository in Azure DevOps.

Solution: Configure the build pipeline to use a Hosted VS 2019 agent pool. Include the Java Tool Installer task in the build pipeline.

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Instead use Octopus Tentacle.

Reference:

https://explore.emtecinc.com/blog/octopus-for-automated-deployment-in-devops-models

Community vote distribution

B (100%)

NKnab Highly Voted 4 years, 1 month ago

The answer is no - https://azuredevopslabs.com/labs/vstsextend/octopus/

upvoted 10 times

vsvaid Most Recent 8 months, 4 weeks ago

Selected Answer: B

No is the answer

upvoted 1 times

gabo 11 months, 3 weeks ago

Doesn't Hosted pool mean "Self-Hosted" pool?

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: B

Use self-hosted agent

Answer is No

upvoted 1 times

UnknowMan 2 years, 4 months ago

Selected Answer: B

Need a self hosted agent

upvoted 1 times

demonite 2 years, 4 months ago

Selected Answer: B

no the ans is self-hosted

upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: B

answer is no, we need to use a self hosted agent

upvoted 1 times

vglearn 3 years, 7 months ago

Answer is No

upvoted 2 times

CristianN 4 years ago

As of today there is no Hosted VS2017 agent pool, the choice is Azure Pipelines which incorporate hosted agent pools

upvoted 2 times

ATS006300 4 years, 3 months ago

The answer is "Yes"

If configured the hosted agent pool will be able to reach the on premise management system

https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/agents?view=azure-devops&tabs=browser

upvoted 3 times

junkz 4 years, 3 months ago

I agree with that, but this extra config step is not mentioned in the answer, so not sure it can automatically be infered

upvoted 1 times

zalyoung 4 years, 2 months ago

Same confusing here, I think enable the Microsoft-hosted agent to access the on-premise dependency is an important setting, but it doesn't mention here. So I will choose No.

upvoted 1 times

jitkv20 4 years, 1 month ago

Sorry I'm starting with Azure devops. Reading through that article too, unless self hosted agent is installed in on-premise system, can we make use of build pipeline there? Here they say its MS hosted 2017 agent right?

upvoted 1 times

Kalaismile06 3 years, 3 months ago

We can't use Hosted VS2017 agent to build Java App. so, the answer is "NO".

upvoted 1 times

Fred64 4 years, 4 months ago

The answer is Yes

upvoted 1 times

Doenoe 4 years, 3 months ago

I dont think the answer is yes, the hosted agent pool would not be able to reach the on premise management system

upvoted 11 times

Duleep 4 years, 1 month ago

agreed with you, answer should be NO, "The builds must access an on-premises dependency management system" hosted agent doesn't have access to on-premiss

upvoted 3 times

Question #10 *Topic 7*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You need to recommend an integration strategy for the build process of a Java application. The solution must meet the following requirements:

- ➪ The builds must access an on-premises dependency management system.
- ➪ The build outputs must be stored as Server artifacts in Azure DevOps.
- ➪ The source code must be stored in a Git repository in Azure DevOps.

Solution: Configure the build pipeline to use a Hosted Ubuntu agent pool. Include the Java Tool Installer task in the build pipeline.

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Instead use Octopus Tentacle.

Reference:

https://explore.emtecinc.com/blog/octopus-for-automated-deployment-in-devops-models

Community vote distribution

B (100%)

ShawInnes Highly Voted 3 years, 7 months ago

It's definitely No. However the alternative given in the description about Octopus is wrong.

upvoted 17 times

syu31svc Highly Voted 2 years, 1 month ago

Selected Answer: B

Use self-hosted agent

Answer is No

upvoted 8 times

UrbanRellik Most Recent 3 months, 2 weeks ago

Selected Answer: B

In cloud computing, when reading about a service offering described to be "Hosted" that would reference the third-party or PaaS provider hosting your application or in this case the MS Hosted Agent.

Context must specify self-hosted agent.

upvoted 1 times

vsvaid 8 months, 4 weeks ago

Selected Answer: B

Agree with answer

upvoted 1 times

gabo 11 months, 3 weeks ago

Unless they use the word, "self-hosted", it should be assumed that "hosted" means Microsoft Hosted so the answers for all such questions will be a NO

upvoted 2 times

debleenac85 2 years, 5 months ago

Octopus is wrong. Let me explain why. First Octopus is a Deployment Tool and the question is about Build Process. Next it's mentioned "Build Artifact's must be stored in Azure DevOps server". If you visit octopus site you will see that here packages are pushed to octopus server package and not azure Artifacts.

Here self hosted agent that "demands" Java will be used.
upvoted 4 times

Pav143 2 months, 4 weeks ago
No, I won't let you explain
upvoted 1 times

Endrit 2 years, 5 months ago
I agree with Jords
upvoted 3 times

rdemontis 2 years, 5 months ago
Selected Answer: B
for me answer is correct but wrong explanation
upvoted 2 times

Whirly 2 years, 6 months ago
Discussion :What if we answer no to all the questions in the set that will give you 3 correct and 1 wrong. it is better than getting 2 correct and 2 wrong?
upvoted 2 times

buzzerboy 1 year, 7 months ago
thats my strategy for these types of questions!
upvoted 2 times

Gluckos 2 years, 7 months ago
Agree with jords
upvoted 2 times

Jords 3 years, 1 month ago
I agree with ScreamingHand
upvoted 4 times

d0bermannn 3 years ago
recursion detected
upvoted 4 times

UnknowMan 2 years, 4 months ago
Agree with jords
upvoted 1 times

shash_ank 2 years, 3 months ago
every now and then i keep seeing, the comment section looks like a reddit comment thread
upvoted 1 times

ScreamingHand 3 years, 1 month ago
I agree with dknagia
upvoted 3 times

ahaz 3 years, 3 months ago
The correct answer is NO, not because the Octopus is the right option, but because the right option is to use a self-hosted agent on an on-prem server
upvoted 5 times

Dsyadav 3 years, 5 months ago
No is correct
upvoted 2 times

vglearn 3 years, 7 months ago
Answer is No
upvoted 6 times

dknangia 3 years, 9 months ago
I agree with OhBee
upvoted 3 times

anujmehta7 4 years, 4 months ago

I think answer is Yes, pls comment

upvoted 2 times

OhBee 4 years, 4 months ago

No. A hosted agent does nor have access to on-prem servers.

upvoted 34 times

Zdujgfr567783ff 2 years, 6 months ago

well you can open (but ip will be random)

also, it is just a build. Once an artifact produced and published, you can download it onpremise

upvoted 1 times

Question #11 *Topic 7*

Your company uses a Git repository in Azure Repos to manage the source code of a web application. The master branch is protected from direct updates.
Developers work on new features in the topic branches.
Because of the high volume of requested features, it is difficult to follow the history of the changes to the master branch.
You need to enforce a pull request merge strategy. The strategy must meet the following requirements:
➪ Consolidate commit histories.
➪ Merge the changes into a single commit.
Which merge strategy should you use in the branch policy?

A. squash merge

B. fast-forward merge

C. Git fetch

D. no-fast-forward merge

Suggested Answer: *A*
Squash merging is a merge option that allows you to condense the Git history of topic branches when you complete a pull request. Instead of each commit on the topic branch being added to the history of the default branch, a squash merge takes all the file changes and adds them to a single new commit on the default branch.
A simple way to think about this is that squash merge gives you just the file changes, and a regular merge gives you the file changes and the commit history.
Note: Squash merging keeps your default branch histories clean and easy to follow without demanding any workflow changes on your team. Contributors to the topic branch work how they want in the topic branch, and the default branches keep a linear history through the use of squash merges. The commit history of a master branch updated with squash merges will have one commit for each merged branch. You can step through this history commit by commit to find out exactly when work was done.
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/git/merging-with-squash

Community vote distribution

AS007 Highly Voted 4 years, 4 months ago
correct answer - verified
upvoted 36 times

Yusho Highly Voted 4 years ago
I agree
upvoted 6 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: A
A. squash merge
upvoted 1 times

vsvaid 8 months, 4 weeks ago
Selected Answer: A
Correct answer
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: A
correct answer
upvoted 1 times

xRiot007 1 year, 1 month ago
squash merge will merge all those commits into one single commit that will be pushed.
Squashing can be good when you have a lot of commits and you want to "condense" things.
upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: A

Squash merging is a merge option that allows you to condense the Git history of topic branches when you complete a pull request

From https://docs.microsoft.com/en-us/azure/devops/repos/git/merging-with-squash?view=azure-devops

A is the answer

upvoted 3 times

UnknowMan 2 years, 4 months ago

Selected Answer: A

Correct => with "squash merge" you can merge all commit together

upvoted 1 times

shash_ank 2 years, 3 months ago

and the commit history of the topic branch gets omitted too

upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: A

correct answer

upvoted 2 times

lugospod 2 years, 7 months ago

Got this January 2022. Squash (got 100% on that part)

upvoted 3 times

Surda 2 years, 8 months ago

Selected Answer: A

Answer is correct

upvoted 2 times

DrewL 3 years, 1 month ago

correct answer, through squash, you can merge multi commits to a single commit

upvoted 4 times

Fred64 4 years, 4 months ago

I agree

upvoted 4 times

Question #12 *Topic 7*

Your company uses cloud-hosted Jenkins for builds.
You need to ensure that Jenkins can retrieve source code from Azure Repos.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Create a webhook in Jenkins.

B. Add the Team Foundation Server (TFS) plug-in to Jenkins.

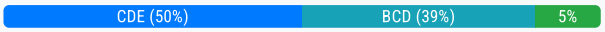
C. Add a personal access token to your Jenkins account.

D. Create a personal access token (PAT) in your Azure DevOps account.

E. Create a service hook in Azure DevOps.

Suggested Answer: *BCD*
B: Jenkins requires a plug-in to connect to TFS and check for updates to a project.
Jenkins' built-in Git Plugin or Team Foundation Server Plugin can poll a Team Services repository every few minutes and queue a job when changes are detected.
C: Use Azure DevOps/ Visual Studio Team Services to create a Personal access token.
D: After you have generated credentials using Visual Studio Team Services, you need to use those credentials in Jenkins.
Reference:
http://www.aisoftwarellc.com/blog/post/how-to-setup-automated-builds-using-jenkins-and-visual-studio-team-foundation-server/2044

Community vote distribution



denisred Highly Voted 3 years, 5 months ago
I think B,D,E are right answers!
upvoted 32 times

ChauPhan 2 years, 10 months ago
Why E? "You need to ensure that Jenkins can retrieve source code from Azure Repos." That's mean Jenkins access to Azure Repo, get the repo and run build. Not from Azure DevOps to trigger Jenkins
1. You need to install something at Jenkins to access Azure Repo --> B
2. Generate PAT at Azure Repo/DevOps --> D
3. Input this PAT at Jenkins to access the repo --> C
upvoted 14 times

zioalex 3 years, 3 months ago
Do not think is correct. B_C_D is. What you should configure a Webhook?
upvoted 6 times

noussa 3 years, 4 months ago
B,D,E
https://devblogs.microsoft.com/devops/vsts-visual-studio-team-services-integration-with-jenkins/
upvoted 3 times

Concay 3 years, 4 months ago
Don't have token how to access?
upvoted 2 times

fflyin2k Highly Voted 3 years, 4 months ago
B,C,D (the given answer is correct)
URL:https://docs.microsoft.com/en-us/azure/developer/jenkins/deploy-to-linux-vm-using-azure-devops-services
by the way, webhook is used for Jenkins + Github, not for Azure Repos.
upvoted 29 times

husam421 Most Recent 2 months, 1 week ago
Selected Answer: BCD
What should you configure as a Webhook?

upvoted 1 times

GPRai 2 months, 3 weeks ago

Selected Answer: CDE

Looks more accurate

upvoted 1 times

ay_m 3 months ago

E Definitely has to be part of the answer, see the link

https://learn.microsoft.com/en-us/azure/devops/service-hooks/services/jenkins?view=azure-devops

upvoted 1 times

UrbanRellik 3 months, 2 weeks ago

Selected Answer: CDE

1) Create a PAT in ADO.

2) Create a service hook subscription in ADO.
https://learn.microsoft.com/en-us/azure/devops/service-hooks/services/jenkins/

3) Add PAT to Jenkins.
https://www.jenkins.io/doc/book/using/using-credentials/

upvoted 1 times

chloaus 5 months ago

Reference for B, D, E as below but it is 4 years ago.
https://github.com/undergroundwires/Azure-in-bullet-points/blob/master/AZ-400%20Microsoft%20Azure%20DevOps%20Solutions/7.3.%20Jenkins.md

upvoted 1 times

FeriAZ 6 months, 1 week ago

Selected Answer: CDE

D. Create a personal access token (PAT) in your Azure DevOps account. (A PAT with read access to the Git repository is still needed for Jenkins to authenticate with Azure DevOps.)
E. Create a service hook in Azure DevOps. (A service hook is crucial to trigger Jenkins builds upon relevant events in Azure DevOps.)
C. Add the Team Foundation Server (TFS) plugin to Jenkins. (While Azure Repos is the current name for the service, the TFS plugin in Jenkins is still compatible and provides the necessary functionality to interact with Azure Repos and clone the source code.)

upvoted 2 times

ozbonny 6 months, 3 weeks ago

Selected Answer: BDE

According with the documentation of the links:
B
D
E
https://learn.microsoft.com/es-es/azure/devops/service-hooks/services/jenkins?view=azure-devops
https://azuredevopslabs.com/labs/vstsextend/jenkins/

upvoted 2 times

vsvaid 8 months, 4 weeks ago

Selected Answer: BCD

I agree with BCD. You do not need to create service hook in Az Devops because we are not triggerring any build. Here we need to Jenkins to access source code from Version control (TFS).

upvoted 2 times

Firdous586 10 months, 2 weeks ago

CDE correct answer already tested in lab

upvoted 2 times

Firdous586 10 months, 3 weeks ago

CDE is Correct checked from Lab

upvoted 2 times

yana_b 10 months, 4 weeks ago

Selected Answer: BCD

https://learn.microsoft.com/en-us/azure/developer/jenkins/deploy-to-linux-vm-using-azure-devops-services

upvoted 1 times

oskarq 11 months, 2 weeks ago

https://learn.microsoft.com/en-us/azure/devops/service-hooks/services/jenkins?view=azure-devops

Here is shows PAT (D),
PAT=API token in Jenkins (C)
service hook in Azure DevOps (E)

upvoted 2 times

Bear_Polar 11 months, 3 weeks ago

Selected Answer: BCD

I think B,C,D are correct. This question requires you to ensure that Jenkins can pull code from your repo (needs PAT + adding PAT to Jenkins + configure plugin) but does not ask to trigger the process after commits or whatever (service hook is not needed). There are more than 3 steps need to be taken in order to make things work.
Ref: https://learn.microsoft.com/en-us/azure/developer/jenkins/deploy-to-linux-vm-using-azure-devops-services

upvoted 1 times

ieboaix 1 year, 1 month ago

CDE https://learn.microsoft.com/en-us/azure/devops/service-hooks/services/jenkins?view=azure-devops

upvoted 2 times

renzoku 1 year, 1 month ago

Selected Answer: BCD

D. Create a PAT in your Azure DevOps account.
Unique identifier and a secret that you can use to authenticate Jenkins with Azure Devops.
Serves as the credentials for Jenkins to access your Azure Repos securely.

B. Add the Team Foundation Server (TFS) plug-in to Jenkins.
Enables Jenkins to communicate with Azure DevOps and allows it to use the created PAT for authentication.

C. Add the PAT to your Jenkins account.
You provide the PAT during the plug-in configuration to allow Jenkins to authenticate itself and access Azure Repos securely.

upvoted 1 times

DRAG DROP -

Your company has four projects. The version control requirements for each project are shown in the following table.

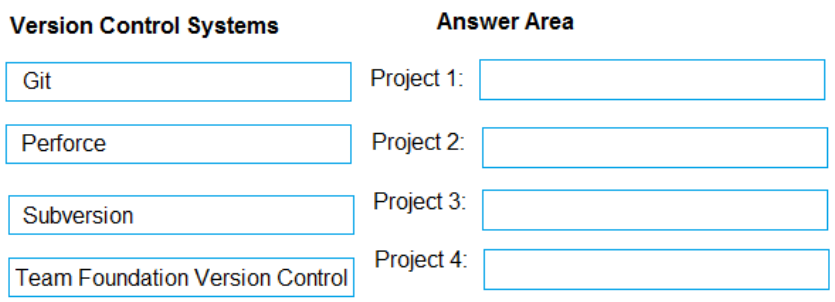
Project	Requirement
Project 1	Project leads must be able to restrict access to individual files and folders in the repository.
Project 2	The version control system must enforce the following rules on the server before merging any changes to the main branch: • Changes must be reviewed by at least two project members. • Changes must be associated by at least one work item
Project 3	The project members must be able to work in Azure Repos directly from Xcode.
Project 4	The release branch must only be viewable or editable by the project leads.

You plan to use Azure Repos for all the projects.

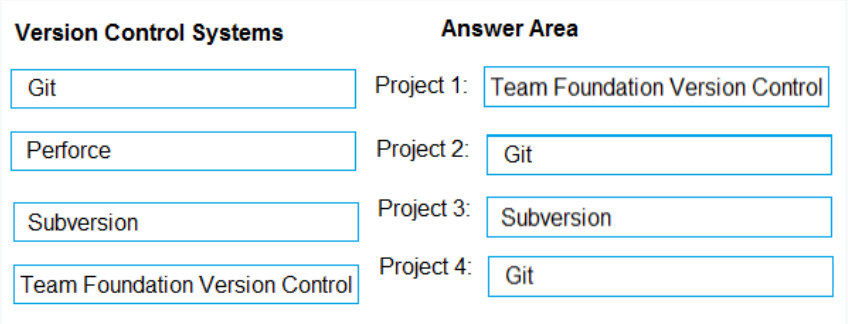
Which version control system should you use for each project? To answer, drag the appropriate version control systems to the correct projects. Each version control system may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested Answer:



Box 1: Team Foundation Version Control

TFVC lets you apply granular permissions and restrict access down to a file level.

Box 2: Git -

Git is the default version control provider for new projects. You should use Git for version control in your projects unless you have a specific need for centralized version control features in TFVC.

Box 3: Subversion -

Note: Xcode is an integrated development environment (IDE) for macOS containing a suite of software development tools developed by Apple

Box 4: Git -

Note: Perforce: Due to its multitenant nature, many groups can work on versioned files. The server tracks changes in a central database of MD5 hashes of file content, along with descriptive meta data and separately retains a master repository of file versions that can be verified through the hashes.

Reference:

https://searchitoperations.techtarget.com/definition/Perforce-Software https://docs.microsoft.com/en-us/azure/devops/repos/git/share-your-code-in-git-xcode https://docs.microsoft.com/en-us/azure/devops/repos/tfvc/overview

denisred Highly Voted 3 years, 5 months ago

TFVS
Git
Git
TFVS
upvoted 48 times

noussa 3 years, 4 months ago

True cause Azure Repos supports only Git and TFVS
https://docs.microsoft.com/en-us/azure/devops/repos/get-started/what-is-repos?view=azure-devops
upvoted 5 times

pavan555manjunath 3 years, 4 months ago

This Answer is correct
TFVS
Git
Git
TFVS
upvoted 9 times

Def21 2 years ago

Correct. Last one: Git Branch Security Permissions and Branch Policies define e.g. editing. Reading is not included
upvoted 1 times

erickim007 Highly Voted 3 years, 3 months ago

the answer should
TFVS
Git
Git
Git
upvoted 13 times

igorole 3 years, 3 months ago

This is not correct as it says "viewable", there is no "read" permissions on a branch. Only:
- Bypass policies when completing pull requests
- Bypass policies when pushing
- Contribute
- Edit policies
- Force push (rewrite history, delete branches and tags)
- Manage permissions
- Remove others' locks
upvoted 4 times

devops100 3 years, 1 month ago

"Set up permissions to control who can read and update the code in a branch on your Git repo"
https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-permissions?view=azure-devops
upvoted 3 times

UrbanRellik Most Recent 3 months, 2 weeks ago

TFVC
Git
Git
Git
upvoted 1 times

vsvaid 8 months, 4 weeks ago

TFVS
Git
Git

Git

We can set read permission for Git branch. https://learn.microsoft.com/en-us/azure/devops/repos/git/branch-permissions?view=azure-devops
---
Set up permissions to control who can read and update the code in a branch on your Git repo. You can set permissions for individual users and groups, and inherit and override permissions as needed from your repo permissions.
upvoted 1 times

varinder82 9 months, 3 weeks ago
After going through all the comments final answer is

TFVS
Git
Git
TFVS
upvoted 1 times

ChadTamanio 11 months, 3 weeks ago
Who the heck uses perforce nowadays?
upvoted 2 times

yana_b 1 year ago
Project 1 -> TFVS -> granular permissions & access restrictions to file level -> https://learn.microsoft.com/en-us/azure/devops/repos/tfvc/what-is-tfvc?view=azure-devops#team-foundation-version-control

Project 2 -> GIT -> branch policy to check for linked WIs, as well as to add reviewers automatically -> https://learn.microsoft.com/en-us/azure/devops/repos/git/branch-policies-overview?view=azure-devop
https://learn.microsoft.com/en-us/azure/devops/repos/git/share-your-code-in-git-xcode?view=azure-devops

Project 3 -> GIT -> how to share your Xcode projects using Azure Repos-> https://learn.microsoft.com/en-us/azure/devops/repos/git/share-your-code-in-git-xcode?view=azure-devops

Project 4 -> GIT -> setup branch permissions to control who can read and update the code in a branch on your Git Repo -> https://learn.microsoft.com/en-us/azure/devops/repos/git/branch-permissions?view=azure-devops
upvoted 6 times

zellck 1 year, 3 months ago
1. TFVS
2. Git
3. Git
4. Git

https://learn.microsoft.com/en-us/azure/devops/repos/tfvc/what-is-tfvc?view=azure-devops#team-foundation-version-control
TFVC lets you apply granular permissions and restrict access down to a file level. Because your team checks all its work into Azure DevOps Server, you can easily audit changes and identify which user checked in a changeset. By using compare and annotate, you can identify the exact changes that they made.

https://learn.microsoft.com/en-us/azure/devops/repos/git/branch-policies-overview?view=azure-devops
The following table summarizes the policies you can define to customize a branch.
- Check for linked work items
Encourage traceability by checking for linked work items on pull requests.
- Automatically included reviewers
Add one or more policies to designate code reviewers to automatically include when pull requests change certain areas of code. Can also enable or disable policies.

https://learn.microsoft.com/en-us/azure/devops/repos/git/share-your-code-in-git-xcode?view=azure-devops
upvoted 6 times

zellck 1 year, 3 months ago
https://learn.microsoft.com/en-us/azure/devops/repos/git/branch-permissions?view=azure-devops
Set up permissions to control who can read and update the code in a branch on your Git repo. You can set permissions for individual users and

groups, and inherit and override permissions as needed from your repo permissions.
upvoted 3 times

Fal991l 1 year, 5 months ago
GPT: Project1: Git - Git is a widely used distributed version control system that is well-suited for managing source code for software development projects. It offers features such as branching and merging, which are useful for managing parallel development efforts. Additionally, Azure Repos supports Git as a version control system, making it a good choice for Project1.
upvoted 1 times

Fal991l 1 year, 5 months ago
Project2: Team Foundation Version Control - Team Foundation Version Control (TFVC) is a centralized version control system that is part of the Azure DevOps suite. It is a good choice for projects that require a more rigid version control structure, such as those with regulatory compliance requirements or those that have a large number of developers working on a single codebase. As Project2 is a hardware development project, it may require a more centralized approach to version control, making TFVC a good choice.
upvoted 1 times

Fal991l 1 year, 5 months ago
Project3: Subversion - Subversion (SVN) is a centralized version control system that is popular in enterprise environments. It is designed to be easy to use and offers features such as versioning, branching, and merging. It is a good choice for projects that require a more structured approach to version control, such as those with a large number of developers working on a single codebase. As Project3 is an enterprise project, Subversion may be a good choice.
upvoted 1 times

Fal991l 1 year, 5 months ago
Project4: Perforce - Perforce is a centralized version control system that is designed for managing large codebases with a large number of developers. It offers features such as branching, merging, and versioning, making it a good choice for complex software development projects. As Project4 is a large software development project, Perforce may be a good choice for version control.
upvoted 1 times

Rams_84zO6n 1 year, 6 months ago
Git, Git, TFVC, Git
https://learn.microsoft.com/en-us/azure/devops/repos/get-started/what-is-repos?view=azure-devops
upvoted 2 times

Rams_84zO6n 1 year, 6 months ago
I think Git, Git, Git, Git is also the right answer
upvoted 2 times

AlexeyG 1 year, 6 months ago
got this in 02 March 2023 exams. scored 870 marks.
upvoted 3 times

armvch 1 year, 6 months ago
We're very happy to know it, Alexey! Maybe you can provide your answer instead?
upvoted 18 times

syu31svc 2 years, 1 month ago
https://docs.microsoft.com/en-us/azure/devops/repos/tfvc/comparison-git-tfvc?view=azure-devops

"You should use Git for version control in your projects and begin to move your existing TFVC projects to Git"

Projects 2, 3 and 4 are Git

https://docs.microsoft.com/en-us/azure/devops/repos/tfvc/comparison-git-tfvc?view=azure-devops

"You can apply permissions at the file level. You can lock files."

Project 1 is TFVS
upvoted 4 times

tjeerd 2 years, 1 month ago
On exam 20220727. Answer is:
TFVS
Git

Git
TFVS
upvoted 9 times

SlavMar 2 years, 4 months ago
There is no option for "pull request" in Git. This functionality is added by system that wraps Git like Bitbucket or Azure DevOps
upvoted 1 times

renzoku 1 year, 2 months ago
Yes, there is.
https://www.atlassian.com/git/tutorials/making-a-pull-request
upvoted 1 times

Cheehp 2 years, 5 months ago
Selected during exam.
TFVS
Git
Git
TFVS
upvoted 7 times

rdemontis 2 years, 5 months ago
It seems that there is a read access also for git repos.
https://docs.microsoft.com/en-us/azure/devops/organizations/security/default-git-permissions?view=azure-devops

In addition the requirement is viewable or editable for the project leads, so i think the answer for project 4 could be Git.
For me correct answer are
1. TFVC
2. Git
3. Git
4. Git
upvoted 3 times

Axz 2 years, 6 months ago
Got this question today March 2022
upvoted 9 times

Whirly 2 years, 6 months ago
Thanks Axz for your comments on question that appeared in exam.
upvoted 5 times

Question #14 *Topic 7*

You are automating the build process for a Java-based application by using Azure DevOps.
You need to add code coverage testing and publish the outcomes to the pipeline.
What should you use?

A. Bullseye Coverage

B. JUnit

C. JaCoCo

D. MSTest

Suggested Answer: *C*
Use Publish Code Coverage Results task in a build pipeline to publish code coverage results to Azure Pipelines or TFS, which were produced by a build in
Cobertura or JaCoCo format.
Incorrect Answers:
A: Bullseye Coverage is used for C++ code, and not for Java.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
➪ Cobertura
➪ JaCoCo
Other incorrect answer options you may see on the exam include the following:
➪ Coverlet
➪ NUnit
➪ Coverage.py
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/test/publish-code-coverage-results

Community vote distribution
C (100%)

denisred Highly Voted 3 years, 5 months ago
Correct!
upvoted 12 times

denisred 3 years, 5 months ago
JaCoCo - JAva COde COverage
upvoted 38 times

UnknowMan 2 years, 4 months ago
Thanks
upvoted 1 times

mohammed159 2 years, 4 months ago
thanks
upvoted 1 times

Kinon4 3 years, 4 months ago
Thanks!
upvoted 6 times

volturyon 3 years, 4 months ago
U ARE WELCOME
upvoted 4 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: C
C. JaCoCo
JaCoCo is a free code coverage library for Java, which has been created by the EclEmma team based on the lessons learned from using and

integration existing libraries for many years

upvoted 1 times

vsvaid 8 months, 4 weeks ago

Selected Answer: C

agree with JCoCo

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: C

https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/test/publish-code-coverage-results?view=azure-devops:

The task supports popular coverage result formats such as Cobertura and JaCoCo.

C is the answer

upvoted 1 times

Eltooth 2 years, 4 months ago

Selected Answer: C

C is correct answer.

upvoted 1 times

Raulgt 2 years, 5 months ago

JUnit is not a possible answer, even though is a set of libraries used in Java that is intended for unit tests only.

upvoted 2 times

anhtvux 1 year, 7 months ago

I still dont get it. Is JUnit not able to measure code coverage to put to the pipeline?

upvoted 2 times

Cheehp 2 years, 5 months ago

Selected during exam.

C. JaCoCo

upvoted 1 times

d0bermannn 2 years, 11 months ago

jcode coverage = JaCoCo or Cobertura

upvoted 1 times

kinqlar 3 years, 1 month ago

Wouldn't JUnit also be possible?

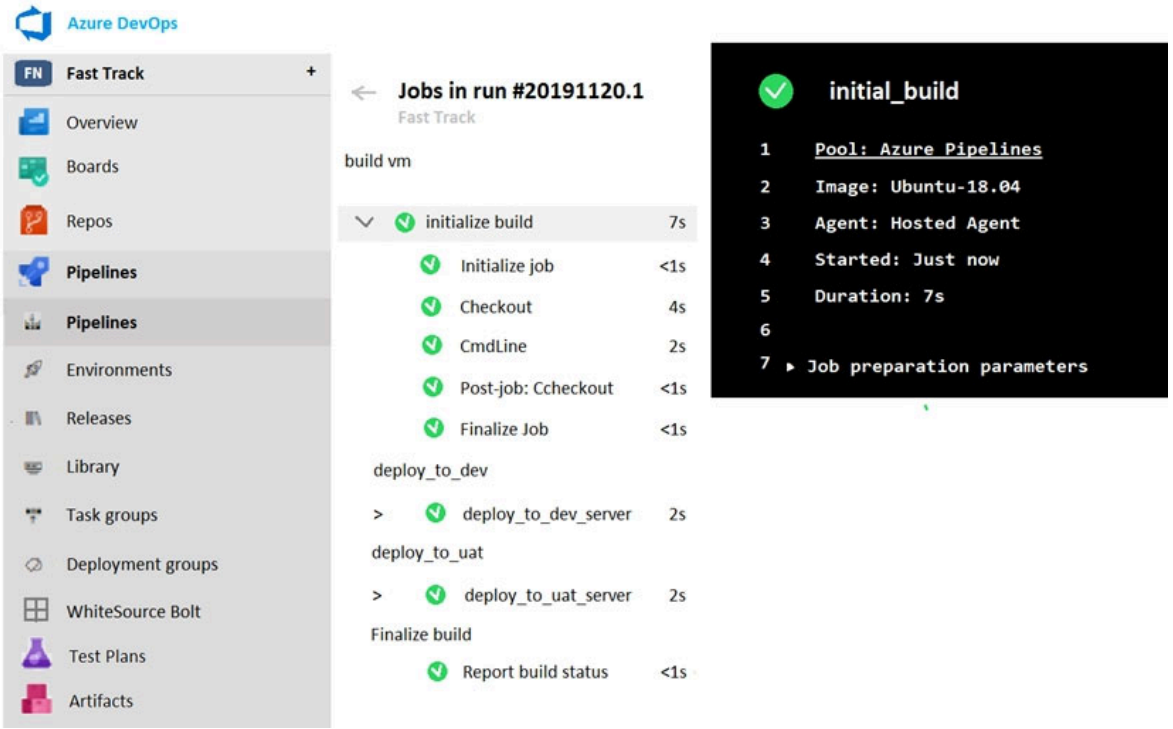
upvoted 1 times

HOTSPOT -

You company uses Azure DevOps to deploy infrastructures to Azure.

Pipelines are developed by using YAML.

You execute a pipeline and receive the results in the web portal for Azure Pipelines as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

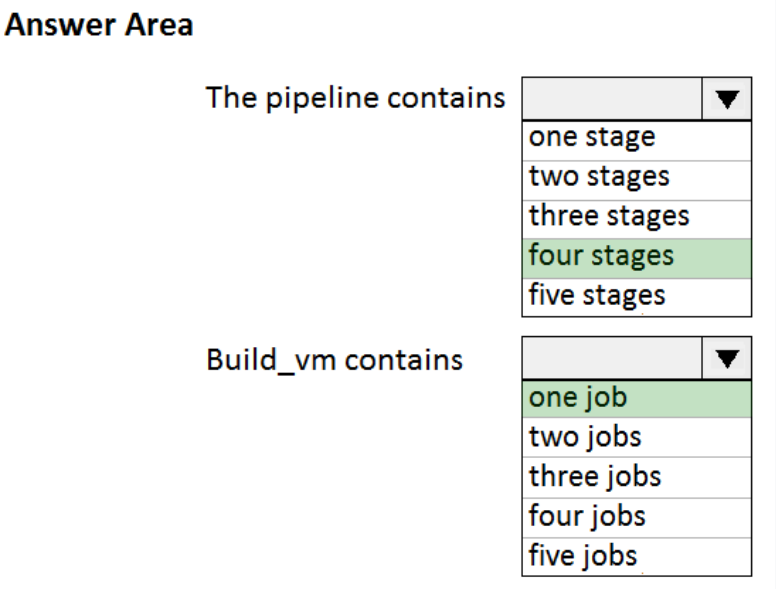
The pipeline contains

- one stage
- two stages
- three stages
- four stages
- five stages

Build_vm contains

- one job
- two jobs
- three jobs
- four jobs
- five jobs

Suggested Answer:



Reference:
https://dev.to/rajikaimal/azure-devops-ci-cd-yaml-pipeline-4glj

chandrakant418 Highly Voted 3 years, 5 months ago
3stage
1 Job
upvoted 73 times

Inland 2 years, 3 months ago
As per AZ-400t00 course material: Stages are the primary divisions in a pipeline: "build the app," "run integration tests," and "deploy to user acceptance testing" are 3 good examples of stages.
upvoted 3 times

ukkuru 3 years, 1 month ago
What are those 3 stages?
upvoted 6 times

zzyy 2 years, 6 months ago
1.Build
2.Deploy to dev
3. Deploy to eat
upvoted 6 times

Raja_v51 2 years, 8 months ago
1-build vm : It has just one job, Initialize Build
2- deploy_to_dev
3-deploy_to_uat
4-Finalize Build -No need to count this Finalize Build stage. It will come automatically to all the pipelines.
upvoted 5 times

demonite 2 years, 4 months ago
wrong - reporting a build status at it's shown it something custom, not automatic - so 4 stages and 1 job
upvoted 7 times

yana_b 1 year, 1 month ago
1 Job, 3 stages (build, deploy to dev, deploy to UAT)
upvoted 2 times

yana_b 1 year ago
Correct answer is 3 stages and 3 jobs.
Reproduced this and after the build stage I get a finalize job task, then after the deploy stage I also got finalize job task. Each job is marked via a green thick sign. You have info about the job preparation parameters. You can also look at the raw log for each of the jobs.
upvoted 1 times

usamnkkid 12 months ago
NO, You are wrong Here. buidl Vm Stage contain only one job which is cmdLine others are by default task.

upvoted 2 times

ahaz Highly Voted 3 years, 3 months ago

The given answer is correct

Stages:

1-build vm : It has just one job, Initialize Build

2- deploy_to_dev

3-deploy_to_uat

4-Finalize Build

upvoted 51 times

sondrex Most Recent 1 month, 4 weeks ago

3stage

1 Job

Three stages: The screenshot shows three distinct stages:

initialize build

deploy_to_dev

deploy_to_uat

Build_vm Contains:

One job: The job shown under initialize build stage includes the following steps:

Initialize job

Checkout

CmdLine

Post-job: Checkout

Finalize Job

These steps are part of a single job execution process.

upvoted 1 times

husam421 2 months, 2 weeks ago

I don't know what is going on here, but there's no stage without jop

upvoted 1 times

mcabrito 6 months, 2 weeks ago

Answer is correct!!

4 stages

1 job

upvoted 1 times

ozbonny 6 months, 3 weeks ago

After further reviewing

I think this has 4 stages 1 job

upvoted 1 times

Predator1NL 8 months, 3 weeks ago

3 stages

3 Jobs

Hierarchy is Stage > Job > Task

See link for info https://dev.to/rajikaimal/azure-devops-ci-cd-yaml-pipeline-4glj

upvoted 2 times

vsvaid 8 months, 4 weeks ago

3 stages

3 job

There is atleast one job in eac stage

upvoted 3 times

4b31a3a 9 months, 2 weeks ago

2 Stages, 4 jobs. The clue is in the expandable >

upvoted 1 times

CirusD 11 months, 2 weeks ago

There are 2 stages: Build and Deploy.

In the Build stage, there is 1 job named Build.

In the Deploy stage, there are 2 jobs: Deploy to Pre-production and Deploy to Production.
So, in total:

There are 2 stages.
There are 3 jobs.
upvoted 1 times

gabo 11 months, 3 weeks ago
The YAML definition should be considered here that would provide the given output, and according to that it will be
3 stages
1 job
upvoted 1 times

tempacc4nk 1 year ago
As per https://learn.microsoft.com/en-us/azure/devops/pipelines/get-started/key-pipelines-concepts?view=azure-devops#stage -

A stage is a logical boundary in the pipeline. It can be used to mark separation of concerns (for example, Build, QA, and production). Each stage contains one or more jobs. When you define multiple stages in a pipeline, by default, they run one after the other. You can specify the conditions for when a stage runs.

So it should be 1 stage and 4 jobs.
upvoted 3 times

xRiot007 1 year, 1 month ago
There are 3 STAGES - build vm, deploy 1, deploy 2, finalize is auto append
The build vm stage has 1 job
upvoted 3 times

kay000001 1 year, 3 months ago
The Finalize/Report Build is automatic and not considered as a job.
The Finalize Job is not considerd a job. It's an automatic indication that the processes have been completed.

You cannot have more stages than jobs. Each job is a process completed with a stage.

I say: 3 stages, 4 jobs.

Reference: https://learn.microsoft.com/en-us/azure/devops/pipelines/create-first-pipeline?view=azure-devops&tabs=java%2Ctfs-2018-2%2Cbrowser
upvoted 1 times

Pamban 1 year, 3 months ago
According to MS documentation, answer would be
3 stages
1 job

Reference: https://learn.microsoft.com/en-us/azure/devops/pipelines/create-first-pipeline?view=azure-devops&tabs=java%2Ctfs-2018-2%2Cbrowser
upvoted 2 times

Pamban 1 year, 2 months ago
please ignore above. answer should be

1 stage
3 jobs
upvoted 1 times

RonZhong 1 year, 5 months ago
3 stages
3 jobs
upvoted 5 times

RonZhong 1 year, 5 months ago

3 stages
3 jobs

This is auto generated:
Finalized build
Report build status
upvoted 2 times

Pamban 1 year, 3 months ago
Please provide an valid answer or reference. this is COMPLETELY wrong!!
upvoted 2 times

Rams_84zO6n 1 year, 6 months ago
what i posted last time is incorrect. It is 3 stages, 3 jobs. Finalize build section is not a stage.
upvoted 3 times

Question #16 *Topic 7*

DRAG DROP -

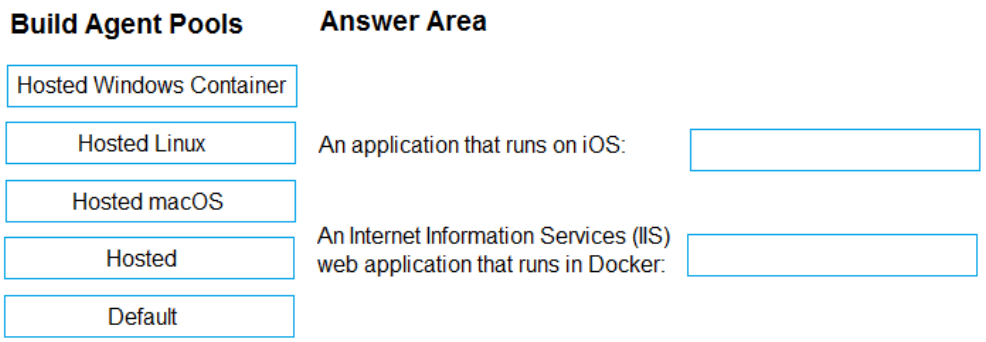
You are configuring Azure DevOps build pipelines.

You plan to use hosted build agents.

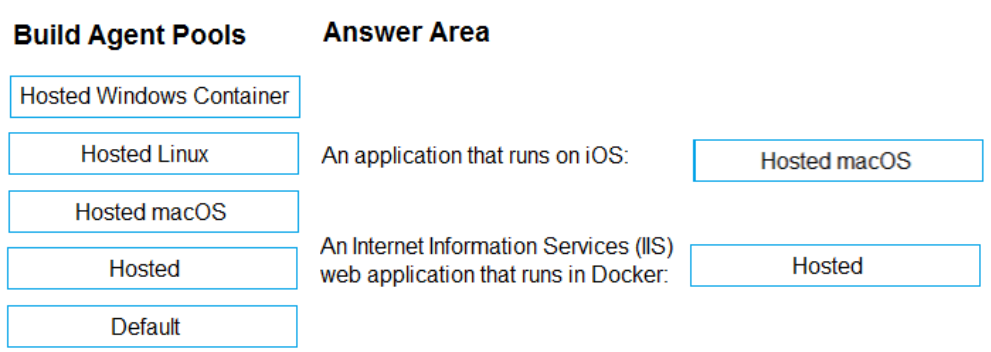
Which build agent pool should you use to compile each application type? To answer, drag the appropriate build agent pools to the correct application types. Each build agent pool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested Answer:



Box 1: Hosted macOS -

Hosted macOS pool (Azure Pipelines only): Enables you to build and release on macOS without having to configure a self-hosted macOS agent. This option affects where your data is stored.

Box 2: Hosted -

Hosted pool (Azure Pipelines only): The Hosted pool is the built-in pool that is a collection of Microsoft-hosted agents.

Incorrect Answers:

Default pool: Use it to register self-hosted agents that you've set up.

Hosted Windows Container pool (Azure Pipelines only): Enabled you to build and release inside Windows containers. Unless you're building using containers,

Windows builds should run in the Hosted VS2017 or Hosted pools.

Hosted Linux/Ubuntu 18.04 does not apply for Mac OS or for Microsoft IIS.

Reference:

https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/agents

Nilf Highly Voted 3 years, 5 months ago

I think

1. Hosted MacOs. See video on https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/hosted?view=azure-devops&tabs=yaml#use-a-microsoft-hosted-agent

2. Hosted

upvoted 35 times

chandrakant418 Highly Voted 3 years, 5 months ago

Hosted for both

upvoted 29 times

chloaus 4 months, 4 weeks ago

The following agent pools are provided by default:
- Default pool: use it to register self-hosted agents.
- Azure Pipelines: hosted pool with various Windows, Linux and macOS images.
https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/pools-queues?view=azure-devops&tabs=yaml%2Cbrowser
- Azure Pipelines agent pool offers several virtual machine images to choose from, including macOS images.
- Microsoft-hosted agents can run jobs directly on the VM or in a container.
https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/hosted?view=azure-devops&tabs=yaml#use-a-microsoft-hosted-agent
- Azure Pipelines can also run Windows Containers. Windows Server version 1803 or higher is required. Docker must be installed.
https://learn.microsoft.com/en-us/azure/devops/pipelines/process/container-phases?view=azure-devops
Azure Pipelines is not available in answers selection.
The next best answer is hosted for both requirements.
upvoted 1 times

ozbonny Most Recent 6 months, 3 weeks ago
1. Hosted MacOs
2. Hosted windows container since not all hosted supports containers
upvoted 1 times

djhyfdgjk 7 months, 1 week ago
Nowadays correct answer should be "Azure Pipelines".
upvoted 1 times

Firdous586 10 months, 3 weeks ago
Answer should be Hosted MAC and Hosted Windows container as its already mentioned IIS is running in Docker engine
upvoted 2 times

dipti927 1 year, 3 months ago
Corrrect Answer is :
1. Hosted MacOs
2. Hosted windows container
upvoted 6 times

Fal991l 1 year, 5 months ago
1. An application that runs on iOS: For building an application that runs on iOS, you should use the **Hosted macOS** build agent pool (Option C). This pool provides a macOS environment with the necessary tools for building iOS applications.

2. An internet Information Services (IIS) web application that runs in Docker: For building an IIS web application that runs in Docker, you should use the **Hosted Windows Container** build agent pool (Option A). This pool provides a Windows environment with support for running Docker containers.

Answers:
1. An application that runs on iOS: c. Hosted macOS
2. An internet Information Services (IIS) web application that runs in Docker: a. Hosted Windows Container
upvoted 9 times

Fal991l 1 year, 5 months ago
GPT: You could use the "Hosted" build agent pool for building an IIS web application that runs in Docker, as this pool provides a Windows-based environment with Docker already installed. However, the "Hosted Windows Container" pool is specifically optimized for building and running Windows containers, so it may provide a more suitable environment for this use case.

So, both "Hosted Windows Container" and "Hosted" could be valid options for the second application type, but "Hosted Windows Container" is more specific to building and running Windows containers, which is the scenario in this case.
upvoted 1 times

warchoon 1 year, 8 months ago
It's always Default now
upvoted 3 times

Frefren 1 year, 8 months ago
1. Hosted MacOS
2. Hosted
"To build and deploy Xcode apps or Xamarin.iOS projects, you'll need at least one macOS agent. This agent can also build and deploy Java and

Android apps."
https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/v2-osx?view=azure-devops
upvoted 2 times

syu31svc 2 years, 1 month ago
I would agree with the given answer

https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/agents?view=azure-devops&tabs=browser

"You can install the agent on Linux, macOS, or Windows machines"

https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/hosted?view=azure-devops&tabs=yaml#use-a-microsoft-hosted-agent
upvoted 3 times

syu31svc 2 years ago
Changed my mind on the IIS application; is Hosted Windows Container

MCQ has one similar question on this and answer is Hosted Windows
upvoted 3 times

xRiot007 1 year, 1 month ago
""You can install the agent on Linux, macOS, or Windows machines" - Correct, but that is not the requirement. The requirement is an IIS application and for that a Hosted Win Container is best.
upvoted 1 times

vikkr 2 years, 1 month ago
https://docs.microsoft.com/ru-ru/azure/devops/pipelines/ecosystems/xcode?view=azure-devops
hosted macos
upvoted 1 times

Matkes 2 years, 1 month ago
The correct answer is hosted for both as they are asking us about the agent pool type which can be only azure pipelines (hosted) and private (self-hosted). Once you will select hosted you will be prompted to provide Agent specifications like: mac, windows ...
upvoted 9 times

cifeng 2 years, 4 months ago
First we need to select Agent pool type, either Hosted or Private.
For Hosted, the choice of agent specifications are: Windows, Linux and MacOS.
upvoted 3 times

UnknowMan 2 years, 4 months ago
1. Hosted (With macos image)
2. Hosted
upvoted 4 times

Optimist_Indian 2 years, 7 months ago
Got this question in Feb-2022 exam (scored 910+). Answered 'Hosted' for both.
upvoted 14 times

lugospod 2 years, 7 months ago
Got this January 2022. Went with hosted Macos and hosted windows...tht total score was above 900 but I dont know if this was correct or not.
upvoted 8 times

binq 2 years, 7 months ago
Hosted for both (https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/hosted?view=azure-devops&tabs=yaml)
upvoted 1 times

Question #17 *Topic 7*

You are automating the build process for a Java-based application by using Azure DevOps.
You need to add code coverage testing and publish the outcomes to the pipeline.
What should you use?

A. Cobertura

B. Bullseye Coverage

C. MSTest

D. Coverlet

Suggested Answer: *A*
Use Publish Code Coverage Results task in a build pipeline to publish code coverage results to Azure Pipelines or TFS, which were produced by a build in
Cobertura or JaCoCo format.
Incorrect Answers:
B: Bullseye Coverage is used for C++ code, and not for Java.
D: If you're building on Linux or macOS, you can use Coverlet or a similar tool to collect code coverage metrics. Code coverage results can be published to the server by using the Publish Code Coverage Results task. To leverage this functionality, the coverage tool must be configured to generate results in Cobertura or
JaCoCo coverage format.
F: Coverage.py is used for Python, not for Java.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. Cobertura
2. JaCoCo
Other incorrect answer options you may see on the exam include the following:
1. Junit
2. NUnit
3. Coverage.py
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/test/publish-code-coverage-results

Community vote distribution

A (100%)

Mefguine Highly Voted 4 years, 4 months ago
Cobertura is a free Java tool that calculates the percentage of code accessed by tests. It can be used to identify which parts of your Java program are lacking test coverage. It is based on jcoverage.
upvoted 6 times

webforce08 Highly Voted 4 years, 9 months ago
Coverlet is a cross platform code coverage framework for .NET. Bullseye Coverage is a code coverage tool for C++.
upvoted 5 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: A
A. Cobertura -> previously asked
upvoted 1 times

Pavlo 1 year, 3 months ago
A. Cobertura
Cobertura is a popular code coverage tool for Java-based applications.
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: A

https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/test/publish-code-coverage-results?view=azure-devops

The task supports popular coverage result formats such as Cobertura and JaCoCo.

A is the answer
upvoted 4 times

Eltooth 2 years, 4 months ago

Selected Answer: A

A is correct answer.
upvoted 2 times

UnknowMan 2 years, 4 months ago

Correct
upvoted 1 times

ArnoudBM 3 years, 9 months ago

Topic 2 question 14 (but without NUnit and Coverage.py as possible answers)
upvoted 2 times

multcloud 3 years, 11 months ago

Cobertura is correct answer
upvoted 2 times

cucuff 4 years, 1 month ago

Answer is A

Cobertura = Java
Coverlet = .NET
Bullseye = C++
upvoted 5 times

zyxphreez 4 years, 2 months ago

coverlet is the tool, cobertura is the format, does anyone have the correct answer?
upvoted 1 times

zyxphreez 4 years, 2 months ago

I changed my answer, I think the correct answer is A, the cobertura was born for Java (Java only), however is a old tool, the coverlet is newer and was develop for .net

projects:
https://cobertura.github.io/cobertura/

https://github.com/coverlet-coverage/coverlet
upvoted 2 times

jmpienqillkaduynay 4 years, 5 months ago

the answer is A
upvoted 3 times

Question #18 *Topic 7*

You have an existing build pipeline in Azure Pipelines.
You need to use incremental builds without purging the environment between pipeline executions.
What should you use?

A. a self-hosted agent

B. Microsoft-hosted parallel jobs

C. a File Transform task

Suggested Answer: *A*
When you run a pipeline on a self-hosted agent, by default, none of the subdirectories are cleaned in between two consecutive runs. As a result, you can do incremental builds and deployments, provided that tasks are implemented to make use of that. You can override this behavior using the workspace setting on the job.
Incorrect Answers:
B: The workspace clean options are applicable only for self-hosted agents. When using Microsoft-hosted agents job are always run on a new agent.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/process/phases

Community vote distribution
A (100%)

SriLen Highly Voted 3 years, 7 months ago
A. Correct Answer
upvoted 17 times

francis6170 Highly Voted 3 years, 2 months ago
Got this in the AZ-400 exam (June 2021).
upvoted 10 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: A
Correct A
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: A
A is correct as supported by given explanation
upvoted 1 times

Eltooth 2 years, 3 months ago
Selected Answer: A
A is correct answer.
upvoted 1 times

UnknowMan 2 years, 4 months ago
Selected Answer: A
Correct
upvoted 2 times

rdemontis 2 years, 5 months ago
Selected Answer: A
correct
upvoted 1 times

nvnrao57 3 years, 4 months ago
Correct
upvoted 2 times

HOTSPOT -

You are designing YAML-based Azure pipelines for the apps shown in the following table.

Name	Platform	Release requirements
App1	Azure virtual machine	Replace a fixed set of existing instances of the previous version of App1 with instances of the new version of the app in each iteration.
App2	Azure Kubernetes Service (AKS) cluster	Roll out a limited deployment of the new version of App2 to validate the functionality of the app. Once testing is successful, expand the rollout.

You need to configure the YAML strategy value for each app. The solution must minimize app downtime.

Which value should you configure for each app? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

App1:
- canary
- rolling
- runonce

App2:
- canary
- rolling
- runonce

Suggested Answer:

Answer Area

App1:
- canary
- rolling
- runonce

App2:
- canary
- rolling
- runonce

App1: rolling -

A rolling deployment replaces instances of the previous version of an application with instances of the new version of the application on a fixed set of virtual machines (rolling set) in each iteration.

App2: canary -

Canary deployment strategy is an advanced deployment strategy that helps mitigate the risk involved in rolling out new versions of applications. By using this strategy, you can roll out the changes to a small subset of servers first. As you gain more confidence in the new version, you can release it to more servers in your infrastructure and route more traffic to it.

Incorrect Answers:

runonce:

runOnce is the simplest deployment strategy wherein all the lifecycle hooks, namely preDeploy deploy, routeTraffic, and postRouteTraffic, are executed once.

Then, either on: success or on: failure is executed.

Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/process/deployment-jobs

Sylph Highly Voted 3 years, 5 months ago
Correct
upvoted 18 times

ozbonny Most Recent 6 months, 3 weeks ago
Correct
upvoted 1 times

renzoku 1 year, 1 month ago
1. Rolling:
Incremental rollout of the new version across all nodes in a controlled manner while minimizing disruption.

2. Canary:
Gradual rollout of new version to a subset of users or nodes
Used to test new features, allowing for risk mitigation and early issue detection.
upvoted 4 times

mamoon_malta2022 2 years ago
A rolling deployment replaces instances of the previous version of an application with instances of the new version of the application on a fixed set of virtual machines (rolling set) in each iteration.
We currently only support the rolling strategy to VM resources.
https://docs.microsoft.com/en-us/azure/devops/pipelines/process/deployment-jobs?view=azure-devops
upvoted 1 times

syu31svc 2 years, 1 month ago
Answer is correct and explanation supports it
upvoted 1 times

hebertpena88 2 years, 1 month ago
Correct
upvoted 1 times

tjeerd 2 years, 1 month ago
On exam 20220727. Answer is correct.
upvoted 3 times

UnknowMan 2 years, 4 months ago
Correct
upvoted 1 times

rdemontis 2 years, 5 months ago
correct
upvoted 2 times

poplovic 3 years, 1 month ago
Rolling for VM, Canary for AKS. One difference is preDeploy is running once for Canary but multiple times for each VM
upvoted 4 times

lesiris 3 years, 2 months ago
Is there a real difference between canary and rolling ? For me they are very similar ...
upvoted 1 times

dupakonia 2 years, 6 months ago
The canary deployment pattern is similar to a rolling deployment in that the IT team makes the new release available to some users before others. However, the canary technique targets certain users to receive access to the new application version, rather than certain servers.
upvoted 5 times

Question #20 *Topic 7*

You have a private project in Azure DevOps.
You need to ensure that a project manager can create custom work item queries to report on the project's progress. The solution must use the principle of least privilege.
To which security group should you add the project manager?

A. Reader

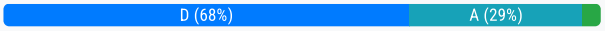
B. Project Collection Administrators

C. Project Administrators

D. Contributor

Suggested Answer: *D*
Contributors have permissions to contribute fully to the project code base and work item tracking. The main permissions they don't have or those that manage or administer resources.
Reference:
https://docs.microsoft.com/en-us/azure/devops/organizations/security/permissions

Community vote distribution



Windscar Highly Voted 3 years, 10 months ago
Answer is correct. There is no reference for shared querires. so its Contributor
upvoted 43 times

Akc0 1 year, 4 months ago
Where did it say shared queries? It mentions principle of least privilege, which in this case is Reader. Others have said a Reader can run the queries without issue.
upvoted 1 times

Akc0 1 year, 4 months ago
I take it back, it should be contributor

Reader > View and run managed queries, view query charts
Contributor > Create and save managed My queries, query charts

Question says they should "Create" queries, reader is not valid boys

https://learn.microsoft.com/en-us/azure/devops/boards/queries/set-query-permissions?view=azure-devops
upvoted 8 times

prgt Highly Voted 3 years, 10 months ago
Answer should be A. Reader
upvoted 20 times

sanhoo 3 years, 1 month ago
igorole has provided the correct explanation.
upvoted 3 times

somenkr 2 years, 5 months ago
Wrong explanation :
https://docs.microsoft.com/en-us/azure/devops/boards/queries/set-query-permissions?view=azure-devops
upvoted 2 times

crutester 3 years, 9 months ago
why???
upvoted 2 times

tom999 3 years, 7 months ago

Because I validated in Azure Boards ;-)
Security group Reader is sufficient to create custom queries and save them under "my queries". BTW: For both access levels: basic and stakeholder
To save "Shared queries" permission group "Project admins" is required, but this is not required in this question.
upvoted 4 times

haxaffee 3 years, 5 months ago
Pretty sure this is right. Look at https://docs.microsoft.com/en-us/azure/devops/boards/queries/about-managed-queries?view=azure-devops#get-started-using-queries -> All valid users with standard access can create queries and folders under the My Queries area. To create queries and query folders under Shared Queries, you must have the Contribute permission set.

Sharing them is not mentioned in the question.
upvoted 1 times

lugospod 2 years, 7 months ago
"All users, except those users assigned to the Readers group, can create and edit their own queries and save them under My Queries."

so the answer must be contributor...

https://docs.microsoft.com/en-us/azure/devops/boards/queries/set-query-permissions?view=azure-devops
upvoted 3 times

igorole 3 years, 2 months ago
It is contributor. See the issue I opened on github:
https://github.com/MicrosoftDocs/azure-devops-docs/issues/10963

Reader has no rights to save anything.
upvoted 28 times

somenkr 2 years, 5 months ago
Reader can save queries
https://docs.microsoft.com/en-us/azure/devops/boards/queries/set-query-permissions?view=azure-devops
upvoted 3 times

binhdortmund 1 year, 8 months ago
readers can save queries somewhere, but not in azure devops.
As it s shown in your link "View and run managed queries, view query charts"
upvoted 1 times

warchoon 1 year, 9 months ago
All users, except those users assigned to the Readers group, can create and edit their own queries and save them under My Queries.
Only the signed in user can view queries saved under their My Queries space.
upvoted 2 times

DevopsRock Most Recent 1 week ago
Selected Answer: D
Answer should be D
upvoted 1 times

UrbanRellik 3 months, 2 weeks ago
Selected Answer: D
https://learn.microsoft.com/en-us/azure/devops/boards/queries/set-query-permissions?view=azure-devops
upvoted 1 times

ozbonny 6 months, 3 weeks ago
Selected Answer: D
D. Contributor
https://learn.microsoft.com/en-us/azure/devops/boards/queries/set-query-permissions?view=azure-devops
upvoted 1 times

vsvaid 8 months, 4 weeks ago
Selected Answer: D
Since the question asks for creating queries, it has to be Contributor. If only running query was needed, then Reader access would have been sufficient.

upvoted 1 times

4b31a3a 9 months, 2 weeks ago

Selected Answer: D

I think report is the keyword. Hard to report on a query that you can't share so it should be contributor.

upvoted 1 times

gabo 11 months, 3 weeks ago

A Reader can save his/her own queries. Since the question doesn't mention the word "Shared". As per least privilege, Reader is the right answer.

upvoted 1 times

gabo 11 months, 3 weeks ago

Ignore what I said, the correct answer is below :

View and run managed queries, view query charts - Reader
Create and save managed My queries, query charts - Contributer

So, a Reader can run a query but cannot save it.

https://learn.microsoft.com/en-us/azure/devops/boards/queries/set-query-permissions?view=azure-devops

upvoted 2 times

gabo 11 months, 3 weeks ago

https://learn.microsoft.com/en-us/azure/devops/boards/queries/about-managed-queries?view=azure-devops

All valid users with standard access can create queries and folders under the My Queries area. To create queries and query folders under Shared Queries, you must have the Contribute permission set.

upvoted 1 times

AymanAkk 11 months, 4 weeks ago

Selected Answer: D

answer is D

upvoted 2 times

yana_b 1 year ago

Selected Answer: D

View and run => Reader
Create My queries => Contributor
Create Shared queries => Project Admin

Question does not refer to shared queries => Contributor

upvoted 2 times

yana_b 1 year ago

evidence can be found here: https://learn.microsoft.com/en-us/azure/devops/boards/queries/set-query-permissions?view=azure-devops

upvoted 1 times

fafda 1 year, 2 months ago

Selected Answer: D

"Create" queries - Contributor.. Reader role can not create query

upvoted 1 times

RealRaymond 1 year, 4 months ago

D Contributor.

https://learn.microsoft.com/en-us/azure/devops/boards/queries/set-query-permissions?view=azure-devops#default-query-permissions

upvoted 1 times

Fal991l 1 year, 5 months ago

Selected Answer: C

GTP: To ensure that a project manager can create custom work item queries to report on the project's progress using the principle of least privilege, you should add the project manager to the Project Administrators security group.

The Project Administrators group is a built-in group in Azure DevOps that has permissions to perform administrative tasks on a project, such as

creating and modifying work item types, managing team members and their permissions, and creating and modifying queries. By adding the project manager to this group, they will have the necessary permissions to create custom work item queries without giving them unnecessary privileges.

On the other hand, adding the project manager to the Reader group would not provide them with the necessary permissions to create custom work item queries, while adding them to the Project Collection Administrators group or Contributor group would give them more privileges than necessary, which goes against the principle of least privilege.

Therefore, the correct answer is C. Project Administrators.
upvoted 1 times

Fal991l 1 year, 5 months ago
You are correct that adding the project manager to the Contributor security group could also be considered as an option that follows the principle of least privilege. As a member of the Contributor group, the project manager would have the permissions necessary to create custom work item queries, and some additional permissions that may be required to perform other tasks related to the project.

However, it's worth noting that the Contributor security group provides more permissions than the Project Administrators group, which is designed specifically for granting administrative permissions within a project. By adding the project manager to the Project Administrators group, you would be granting them only the permissions necessary to perform their duties related to work item queries and not any additional permissions that may not be needed.
upvoted 1 times

Fal991l 1 year, 5 months ago
here are some examples of additional permissions that the Contributor security group provides beyond what is necessary for creating custom work item queries:

Ability to add, modify, or delete resources such as pipelines, builds, releases, repositories, and other project artifacts.
Ability to modify project-level security settings, such as adding or removing security groups, changing project-level permissions, or changing security settings for individual resources within the project.
upvoted 1 times

Fal991l 1 year, 5 months ago
The Project Administrators group provides administrative permissions within a single project, such as the ability to create and manage work items, queries, boards, backlogs, iterations, and other project-level settings. This group does not have administrative permissions outside of the project.
upvoted 1 times

noip 1 year, 7 months ago
A. Reader is Correct. The correct security group to add the project manager to is "Reader". This group provides the minimum necessary permissions for the project manager to create custom work item queries and view project information, while following the principle of least privilege. "Reader" provides the ability to view project information and run saved queries, but does not provide the ability to make changes to the project or its artifacts.
upvoted 1 times

chingdm 1 year, 8 months ago
Answer: Contributor
"All users, except those users assigned to the Readers group, can create and edit their own queries and save them under My Queries. Only the signed in user can view queries saved under their My Queries space."

https://learn.microsoft.com/en-us/azure/devops/boards/queries/set-query-permissions?view=azure-devops
upvoted 1 times

Sam90765 1 year, 8 months ago
Selected Answer: C
His role is called project admin guys. Reader will help him create his own queries but not to share it.
upvoted 1 times

LGWJ12 1 year, 9 months ago
Selected Answer: D
The answer is D, as a reader, you can only run queries, not create them.
upvoted 1 times

Question #21 *Topic 7*

Your company has a project in Azure DevOps for a new application. The application will be deployed to several Azure virtual machines that run Windows Server
2019.
You need to recommend a deployment strategy for the virtual machines. The strategy must meet the following requirements:
➪ Ensure that the virtual machines maintain a consistent configuration.
➪ Minimize administrative effort to configure the virtual machines.
What should you include in the recommendation?

A. Azure Resource Manager templates and the PowerShell Desired State Configuration (DSC) extension for Windows

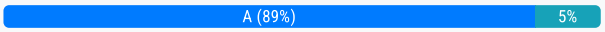
B. Deployment YAML and Azure pipeline deployment groups

C. Azure Resource Manager templates and the Custom Script Extension for Windows

D. Deployment YAML and Azure pipeline stage templates

Suggested Answer: *C*
The Custom Script Extension downloads and executes scripts on Azure virtual machines. This extension is useful for post deployment configuration, software installation, or any other configuration or management tasks. Scripts can be downloaded from Azure storage or GitHub, or provided to the Azure portal at extension run time. The Custom Script Extension integrates with Azure Resource Manager templates, and can be run using the Azure CLI, PowerShell, Azure portal, or the Azure Virtual Machine REST API.
Incorrect Answers:
B: YAML doesn't work with Azure pipeline deployment groups.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/custom-script-windows

Community vote distribution



Root_Access Highly Voted 4 years, 3 months ago
its A: PS DSC. CSE only runs a script and doesnt check for consistency. DSC "Maintains" consistency by regularly checking the target.
upvoted 96 times

kaikailiang 4 years, 3 months ago
Agree, A is correct
upvoted 22 times

lugospod Highly Voted 2 years, 7 months ago
Got this January 2022. A.
upvoted 6 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: C
Previously asked
C. Azure Resource Manager templates and the Custom Script Extension for Windows
reduce administrative effort
upvoted 1 times

vsvaid 8 months, 4 weeks ago
Selected Answer: A
Agree with A
upvoted 1 times

ObiWan500 10 months, 1 week ago
Selected Answer: B
https://learn.microsoft.com/en-us/azure/devops/pipelines/release/deployment-groups/deploying-azure-vms-deployment-groups?view=azure-devops
upvoted 1 times

yana_b 1 year, 1 month ago

Selected Answer: A

It is A

How do I seamlessly set a new desired configuration for all or a subset of my machines? -> follow the url below

https://azure.microsoft.com/en-us/blog/what-why-how-azure-automation-desired-state-configuration/

upvoted 1 times

yana_b 1 year ago

https://purple.telstra.com/blog/arm-custom-script-extension-vs-desired-state-configuration-exten

On this URL it is clearly mentioned that DSC is more efforts consuming than CSE.

upvoted 1 times

Pavlo 1 year, 3 months ago

A. Azure Resource Manager templates and the PowerShell Desired State Configuration (DSC) extension for Windows

This is the correct recommendation.

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: A

"consistent configuration"

This is A to me; DSC

upvoted 3 times

Eltooth 2 years, 4 months ago

Selected Answer: A

A is correct answer.

upvoted 1 times

demonite 2 years, 4 months ago

For A: create ARM template; write a PoSH DSC script; create Automation Account; configure AA; onboard VM

For B: create YAML pipeline; write PoSH DSC script; schedule the pipeline to run every say 10 mins.

Which is less Administrative effort? B

upvoted 1 times

demonite 2 years, 4 months ago

Ideally I'd do Policy DSC which avoids the need for automation accounts.

https://docs.microsoft.com/en-us/azure/governance/policy/concepts/guest-configuration

upvoted 1 times

armvch 1 year, 6 months ago

Option B doesn't contain all of that. It's just "YAML pipeline". So the answer is A.

upvoted 1 times

UnknowMan 2 years, 4 months ago

Selected Answer: A

ARM + DSC

upvoted 2 times

rdemontis 2 years, 5 months ago

Selected Answer: A

Absolutely we need DSC and an azure automation account to maintain consistency. CSE runs only one time.

upvoted 2 times

cannibalcorpse 2 years, 7 months ago

Selected Answer: A

We need DSC

upvoted 2 times

Shreyans 2 years, 7 months ago

Selected Answer: A

A is right answer

upvoted 2 times

Art3 2 years, 7 months ago

A is correct.

upvoted 1 times

darsh19 2 years, 8 months ago

Selected Answer: A

As Root_Access said:

its A: PS DSC. CSE only runs a script and doesnt check for consistency. DSC "Maintains" consistency by regularly checking the target.

upvoted 1 times

ixl2pass 2 years, 8 months ago

A

https://azure.microsoft.com/en-us/blog/what-why-how-azure-automation-desired-state-configuration/

upvoted 1 times

Question #22 *Topic 7*

You have an Azure DevOps project that uses many package feeds.
You need to simplify the project by using a single feed that stores packages produced by your company and packages consumed from remote feeds. The solution must support public feeds and authenticated feeds.
What should you enable in DevOps?

A. Universal Packages

B. upstream sources

C. views in Azure Artifacts

D. a symbol server

Suggested Answer: *B*
Upstream sources enable you to use a single feed to store both the packages you produce and the packages you consume from "remote feeds". This includes both public feeds, such as npmjs.com and nuget.org, and authenticated feeds, such as other Azure DevOps feeds in your organization. Once you've enabled an upstream source, any user connected to your feed can install a package from the remote feed, and your feed will save a copy.
Reference:
https://azure.microsoft.com/en-us/blog/deep-dive-into-azure-artifacts/

Community vote distribution

B (100%)

ttyenJames Highly Voted 3 years, 5 months ago
B. upstream sources
https://docs.microsoft.com/en-us/azure/devops/artifacts/how-to/set-up-upstream-sources?view=azure-devops
upvoted 12 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: B
B. upstream sources
upvoted 1 times

vsvaid 8 months, 4 weeks ago
Selected Answer: B
Agree with B
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: B
B is correct as supported by given explanation
upvoted 2 times

Eltooth 2 years, 4 months ago
Selected Answer: B
B is correct answer.
upvoted 1 times

UnknowMan 2 years, 4 months ago
Correct when you add a new feed you can enable "Include Upstream source"
upvoted 1 times

rdemontis 2 years, 5 months ago
Selected Answer: B
correct answer
upvoted 1 times

agueda 3 years, 7 months ago
Correct answer
Ref: https://docs.microsoft.com/en-us/azure/devops/artifacts/concepts/upstream-sources?view=azure-devops

upvoted 2 times

SriLen 3 years, 7 months ago

B. Correct Answer

upvoted 2 times

Question #23 *Topic 7*

DRAG DROP -

Your company has two virtual machines that run Linux in a third-party public cloud.

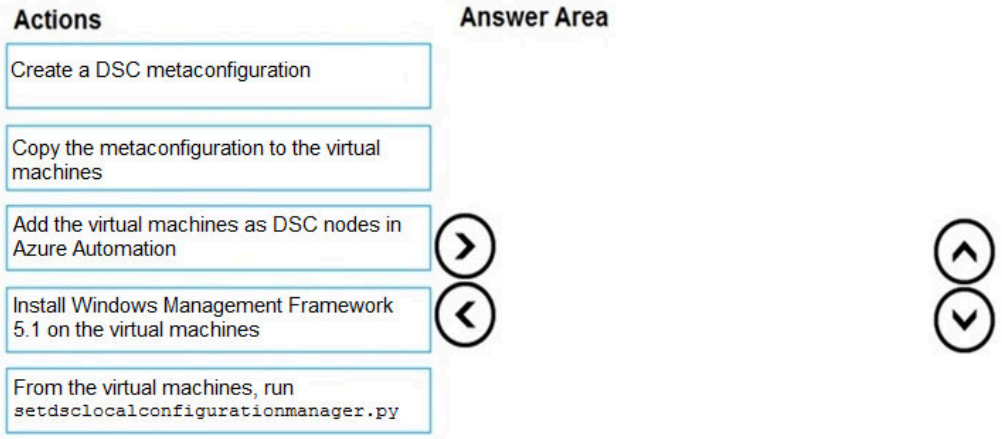
You plan to use the company's Azure Automation State Configuration implementation to manage the two virtual machines and detect configuration drift.

You need to onboard the Linux virtual machines.

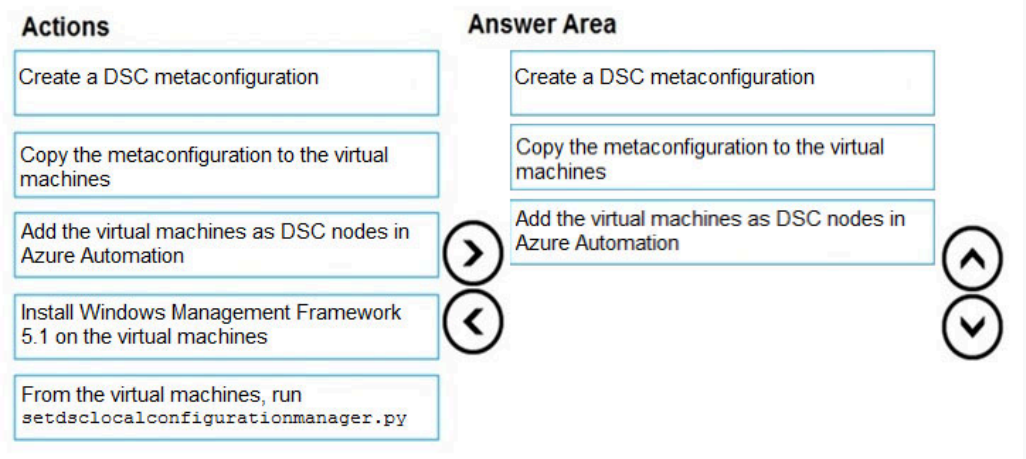
You install PowerShell Desired State Configuration (DSC) on the virtual machines, and then run register.py.

Which three actions should you perform next in sequence? To answer, move the actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Suggested Answer:



Step 1: Create a DSC metaconfiguration

Load up the DSC Configuration into Azure Automation.

Step 2: Copy the metaconfiguration to the virtual machines.

Linking the Node Configuration to the Linux Host

Step 3: Add the virtual machines as DSC nodes in Azure Automation. go to DSC Nodes, select your node, and then click Assign node configuration. This step assigns the DSC configuration to the Linux machine.

Next up will be to link the node configuration to the host. Go to the host and press the ı€Assign nodeı¦€ı€-button. Next up you can select your node configuration.

Sylph Highly Voted 3 years, 5 months ago

Create a DSC metaconfiguration

Copy the metaconfiguration to the virtual machines

From the virtual machines, run setdsclocalconfigurationmanager.py

https://docs.microsoft.com/en-us/azure/automation/automation-dsc-onboarding#enable-physicalvirtual-linux-machines

upvoted 61 times

d0bermannn 2 years, 11 months ago

+ no need to add vms as dsc nodes since we have installed PowerShell Desired State Configuration (DSC) on the virtual machines and ran register.py already.

upvoted 4 times

Amrx 2 years, 2 months ago
Steps 4, 6/7 and 8 in that article make it clear that this is the correct answer, there should be no further argument about this.
upvoted 2 times

rdemontis 2 years, 5 months ago
Yours is the correct answer
upvoted 1 times

Ashutosh_9608 2 years, 11 months ago
correct Sylph
https://docs.microsoft.com/en-us/azure/automation/automation-dsc-onboarding
upvoted 3 times

Optimist_Indian Highly Voted 2 years, 7 months ago
Got this question in Feb-2022 exam.
upvoted 9 times

Yindave Most Recent 4 months, 3 weeks ago
(not shure if it matters as the exam will be renewed the 4th of May)
Got this in the exam today(26-04-2024)
awnsered it wrong but still passed, ha!
upvoted 3 times

vsvaid 8 months, 4 weeks ago
As mentioned by many others, I agree to

1. Create DSC metaconfiguration
2. Copy metaconfiguration to VMs
3. Run setdsclocalconfigurationmanager.py
upvoted 1 times

yana_b 1 year ago
Answer provided by zellck is correct and is evidenced by the link mentioned by that user.
upvoted 1 times

zellck 1 year, 3 months ago
1. Create DSC metaconfiguration
2. Copy metaconfiguration to VMs
3. Run setdsclocalconfigurationmanager.py

https://learn.microsoft.com/en-us/azure/automation/automation-dsc-onboarding#enable-physicalvirtual-linux-machines
- If you can't apply the PowerShell DSC metaconfigurations remotely, copy the metaconfigurations corresponding to the remote machines from the folder to the Linux machines.
- Add code to call Set-DscLocalConfigurationManager.py locally on each Linux machine to enable for State Configuration.
upvoted 5 times

Fal991l 1 year, 5 months ago
Given answers are right. It's backed by GPT.
upvoted 1 times

Fal991l 1 year, 5 months ago
The correct sequence of actions for onboarding the Linux virtual machines using Azure Automation State Configuration and PowerShell DSC would be:

Create a DSC metaconfiguration: The first step is to create a DSC metaconfiguration file that defines the desired state of the virtual machines. The metaconfiguration file should include the configuration settings that you want to apply to the virtual machines, as well as any necessary dependencies or resources.

Copy the metaconfiguration to the virtual machines: Once the metaconfiguration file has been created, it needs to be copied to the virtual machines that you want to manage. You can use a variety of methods to copy the file, such as SCP or SFTP.

Add the virtual machines as DSC nodes in Azure Automation: After the metaconfiguration file has been copied to the virtual machines, you

need to add them as DSC nodes in Azure Automation. This allows Azure Automation to communicate with the virtual machines and apply the desired configuration settings.
upvoted 2 times

Fal991l 1 year, 5 months ago
The other options listed in the question are:

Install Windows Management Framework 5.1 on the virtual machines: This option is not necessary, as Windows Management Framework is a set of tools that is used to manage Windows-based systems, and is not required for Linux-based systems.

From the virtual machines, run setdsclocalconfigurationmanager.py: This option is also not necessary, as the virtual machines have already been registered with Azure Automation using the register.py script. Running setdsclocalconfigurationmanager.py on the virtual machines is used to configure the local DSC settings, which have already been configured in the DSC metaconfiguration file.
upvoted 1 times

AlexeyG 1 year, 6 months ago
got this in 02 March 2023 exams. scored 870 marks.
upvoted 4 times

syu31svc 2 years, 1 month ago
https://docs.microsoft.com/en-us/azure/automation/automation-dsc-onboarding#enable-physicalvirtual-linux-machines

"Follow the directions in Generate DSC metaconfigurations section to produce a folder containing the required DSC metaconfigurations.

Add code as follows to apply the PowerShell DSC metaconfigurations remotely to the machines to enable.

Add code to call Set-DscLocalConfigurationManager.py"

1) Create DSC
2) Copy metaconfiguration
3) Run the .py script
upvoted 1 times

Mev4953 2 years, 6 months ago
https://docs.microsoft.com/en-us/powershell/dsc/getting-started/lnxgettingstarted?view=dsc-1.1#:~:text=SetDscLocalConfigurationManager.py,localhost.meta.mof
upvoted 1 times

meetj 2 years, 11 months ago
Given answer is right, step of "run setdscxxx " is for on-premise only
upvoted 1 times

victor90 2 years, 10 months ago
I don't think so. From the link below, it clearly states it supports third party cloud as well.
The question also mention about third party cloud.
https://docs.microsoft.com/en-us/azure/automation/automation-dsc-onboarding#enable-physicalvirtual-windows-machines
upvoted 2 times

erico 3 years, 2 months ago
Here the first step would be to create the DSC metaconfiguration
Then copy the configuration to the remote machine
And then run the setdsclocalconfigurationmanager.py file to apply the state configuration
upvoted 4 times

SIMULATION -

You plan to deploy a runbook that will create Azure AD user accounts.

You need to ensure that runbooks can run the Azure PowerShell cmdlets for Azure Active Directory.

To complete this task, sign in to the Microsoft Azure portal.

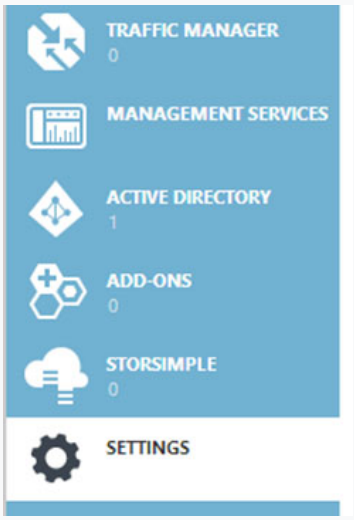
Suggested Answer: *See explanation below.*

Azure Automation now ships with the Azure PowerShell module of version 0.8.6, which introduced the ability to non-interactively authenticate to Azure using OrgId

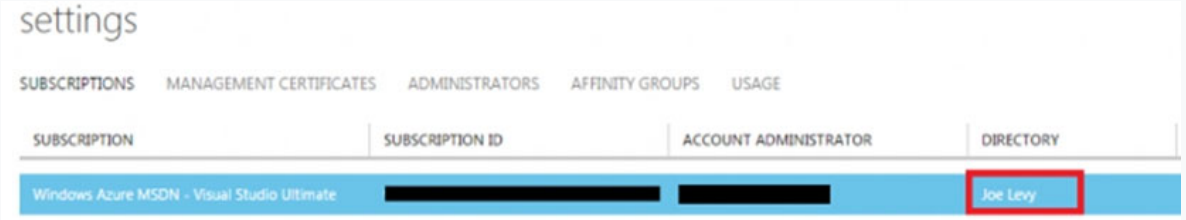
(Azure Active Directory user) credential-based authentication. Using the steps below, you can set up Azure Automation to talk to Azure using this authentication type.

Step 1: Find the Azure Active Directory associated with the Azure subscription to manage:

1. Log in to the Azure portal as the service administrator for the Azure subscription you want to manage using Azure Automation. You can find this user by logging in to the Azure portal as any user with access to this Azure subscription, then clicking Settings, then Administrators.



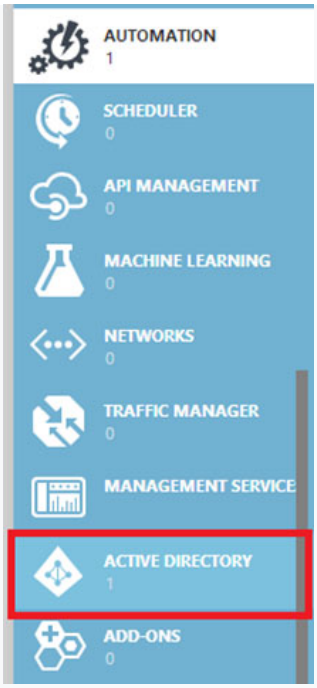
2. Note the name of the directory associated with the Azure subscription you want to manage. You can find this directory by clicking Settings, then Subscriptions.



Step 2: Create an Azure Active Directory user in the directory associated with the Azure subscription to manage:

You can skip this step if you already have an Azure Active Directory user in this directory. and plan to use this OrgId to manage Azure.

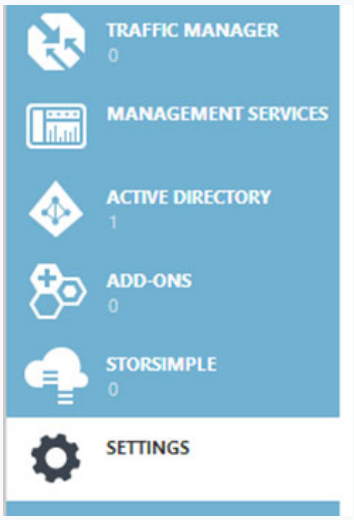
1. In the Azure portal click on Active Directory service.



2. Click the directory name that is associated with this Azure subscription.
3. Click on the Users tab and then click the Add User button.
4. For type of user, select ı€New user in your organization.ı€ Enter a username for the user to create.
5. Fill out the user's profile. For role, pick ı€User.ı€ Don't enable multi-factor authentication. Multi-factor accounts cannot be used with Azure Automation.
6. Click Create.
7. Jot down the full username (including part after @ symbol) and temporary password.

Step 3: Allow this Azure Active Directory user to manage this Azure subscription.

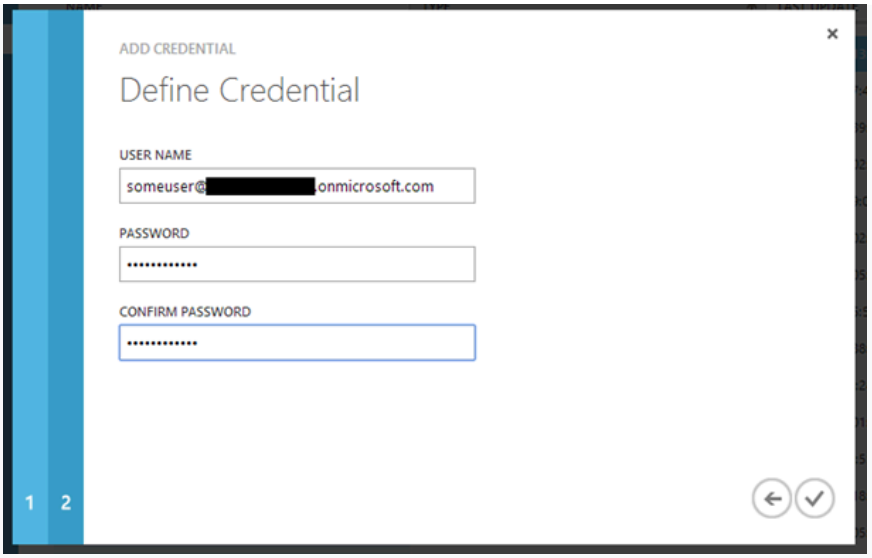
1. Click on Settings (bottom Azure tab under StorSimple)



2. Click Administrators
3. Click the Add button. Type the full user name (including part after @ symbol) of the Azure Active Directory user you want to set up to manage Azure. For subscriptions, choose the Azure subscriptions you want this user to be able to manage. Click the check mark.

Step 4: Configure Azure Automation to use this Azure Active Directory user to manage this Azure subscription

Create an Azure Automation credential asset containing the username and password of the Azure Active Directory user that you have just created. You can create a credential asset in Azure Automation by clicking into an Automation Account and then clicking the Assets tab, then the Add Setting button.



Note: Once you have set up the Azure Active Directory credential in Azure and Azure Automation, you can now manage Azure from Azure Automation runbooks using this credential.
Reference:
https://azure.microsoft.com/sv-se/blog/azure-automation-authenticating-to-azure-using-azure-active-directory/

poplovic Highly Voted 2 years, 12 months ago
The ask is to install AzureAD powershell module for the automation runbooks.
1. select the Automation account with the runbook
2. select Modules, the "browse gallery"
3. search "AzureAD" and install it
upvoted 21 times

rdemontis 2 years, 5 months ago
agree with you
upvoted 1 times

Gabsyfire 7 months, 1 week ago
Just checked now, and that is the perfect answer
upvoted 1 times

Optimist_Indian Highly Voted 2 years, 7 months ago
No simulation question in Feb-2022 exam.
upvoted 10 times

eliisiita1 1 year, 9 months ago
did you take the exam at home?
upvoted 3 times

rints Most Recent 2 years, 6 months ago
Took exam today. 8 lab questions were there, so better to practise all simulation questions as well.
upvoted 10 times

itworxx 3 years, 2 months ago
You need to ensure that runbooks can run the Azure PowerShell cmdlets for Azure Active Directory.
Add the AzureAD PowerShell Module to the modules section in the automation account.
Done.
Credential Object is not a requirement based on the task required.
upvoted 8 times

Sylph 3 years, 5 months ago
https://docs.microsoft.com/en-us/azure/automation/automation-use-azure-ad
upvoted 1 times

DRAG DROP -

You are creating a container for an ASP.NET Core app.

You need to create a Dockerfile file to build the image. The solution must ensure that the size of the image is minimized.

How should you configure the file? To answer, drag the appropriate values to the correct targets. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Values

- `dotnet publish -c Release -o out`
- `dotnet restore`
- `mcr.microsoft.com/dotnet/aspnet:5.0`
- `mcr.microsoft.com/dotnet/sdk:5.0`

Anser Area

```
FROM [ Value ] AS build-env
COPY . /app/
WORKDIR /app
RUN [ Value ]
FROM [ Value ]
COPY --from=build-env /app/out /app
WORKDIR /app
ENTRYPOINT ["dotnet", " MvcMovie.dll"]
```

Suggested Answer:

Values

- `dotnet publish -c Release -o out`

Anser Area

```
FROM [ mcr.microsoft.com/dotnet/sdk:5.0 ] AS build-env
COPY . /app/
WORKDIR /app
RUN [ dotnet restore ]
FROM [ mcr.microsoft.com/dotnet/aspnet:5.0 ]
COPY --from=build-env /app/out /app
WORKDIR /app
ENTRYPOINT ["dotnet", " MvcMovie.dll"]
```

Box 1: mcr.microsoft.com/dotnet/sdk:5.0

The first group of lines declares from which base image we will use to build our container on top of. If the local system does not have this image already, then docker will automatically try and fetch it. The mcr.microsoft.com/dotnet/core/sdk:5.0 comes packaged with the .NET core 5.0 SDK installed, so it's up to the task of building ASP .NET core projects targeting version 5.0

Box 2: dotnet restore -

The next instruction changes the working directory in our container to be /app, so all commands following this one execute under this context.

COPY *.csproj ./

RUN dotnet restore -

Box 3: mcr.microsoft.com/dotnet/aspnet:5.0

When building container images, it's good practice to include only the production payload and its dependencies in the container image. We don't want the .NET core SDK included in our final image because we only need the .NET core runtime, so the dockerfile is written to use a temporary container that is packaged with the SDK called build-env to build the app.

Reference:

https://docs.microsoft.com/en-us/virtualization/windowscontainers/quick-start/building-sample-app

firewind Highly Voted 2 years, 4 months ago

Second field should be dotnet publish -c Release -o out

upvoted 40 times

Angrl 2 years, 4 months ago

Agree with firewind

```
FROM mcr.microsoft.com/dotnet/core/sdk:2.1 AS build-env
WORKDIR /app

COPY *.csproj ./
RUN dotnet restore

COPY . ./
RUN dotnet publish -c Release -o out

FROM mcr.microsoft.com/dotnet/core/aspnet:2.1
WORKDIR /app
COPY --from=build-env /app/out .
ENTRYPOINT ["dotnet", "asp-net-getting-started.dll"]
```

upvoted 4 times

kennynelcon 2 years, 2 months ago

You are right, maybe an error from Examtopics, cos link here is ok

https://docs.microsoft.com/en-us/virtualization/windowscontainers/quick-start/building-sample-app

upvoted 1 times

tjeerd Highly Voted 2 years, 1 month ago

On exam 20220727. Answer is:

SDK

dotnet publish

ASPnet

upvoted 7 times

varinder82 Most Recent 9 months, 3 weeks ago

Final answer after going through all the comments

1. /sdk
2. dotnet publish -c Release -o out
3. /aspnet

upvoted 4 times

CirusD 11 months, 2 weeks ago

```
FROM mcr.microsoft.com/dotnet/aspnet:sdk AS build-env
WORKDIR /app

# Copy csproj and restore as distinct layers
COPY *.csproj ./
RUN dotnet restore

# Copy everything else and build
COPY . ./
RUN dotnet publish -c Release -o out

# Build runtime image
FROM mcr.microsoft.com/dotnet/aspnet:runtime
WORKDIR /app
COPY --from=build-env /app/out .
ENTRYPOINT ["dotnet", "YourApp.dll"]
```

upvoted 1 times

pamswam 1 year, 12 months ago

for second: dotnet publish -c Release -o out (publish do implicit restore)

https://learn.microsoft.com/en-us/dotnet/core/tools/dotnet-publish#description

upvoted 4 times

syu31svc 2 years, 1 month ago

Run dotnet publish -c Release -o out

https://docs.microsoft.com/en-us/virtualization/windowscontainers/quick-start/building-sample-app

Other options are correct

upvoted 2 times

htahara 2 years, 2 months ago

FROM mcr.microsoft.com/dotnet/core/sdk:5.0 AS build-env

RUN dotnet publish -c Release -o out

FROM mcr.microsoft.com/dotnet/aspnet:5.0

upvoted 1 times

UnknowMan 2 years, 4 months ago

Sdk to build

Publish on Out folder

aspnet to run

upvoted 2 times

Question #26 *Topic 7*

DRAG DROP -

You are configuring the settings of a new Git repository in Azure Repos.

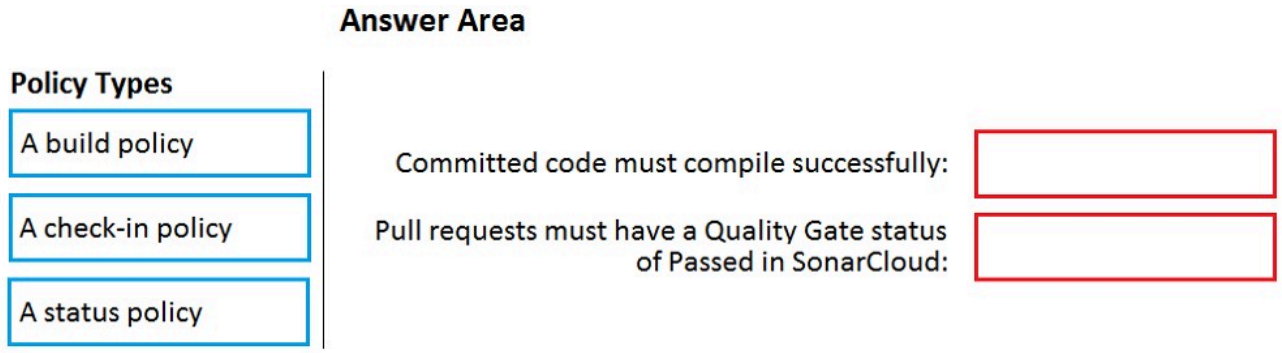
You need to ensure that pull requests in a branch meet the following criteria before they are merged:

- Committed code must compile successfully.
- Pull requests must have a Quality Gate status of Passed in SonarCloud.

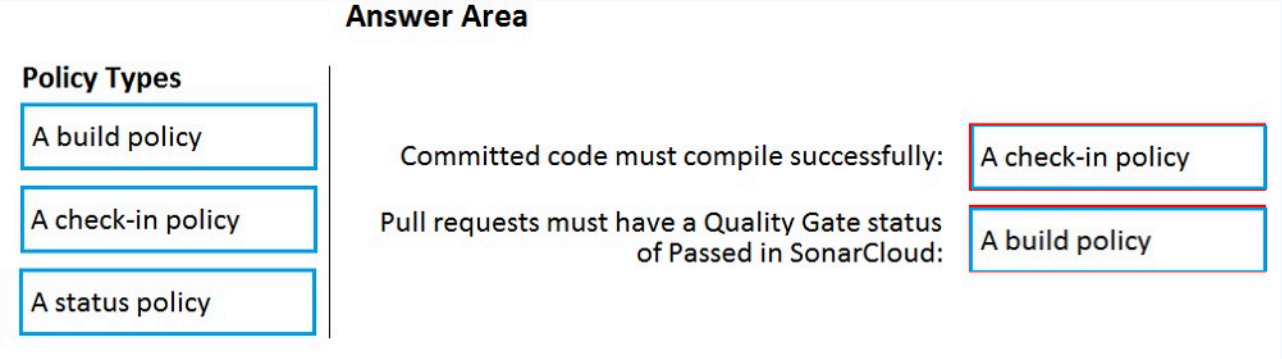
Which policy type should you configure for each requirement? To answer, drag the appropriate policy types to the correct requirements. Each policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested Answer:



Box 1: A check-in policy -

Administrators of Team Foundation version control can add check-in policy requirements. These check-in policies require the user to take actions when they conduct a check-in to source control.

By default, the following check-in policy types are available:

- Builds Requires that the last build was successful before a check-in.
- Code Analysis Requires that code analysis is run before check-in.
- Work Items Requires that one or more work items be associated with the check-in.

Box 2: Build policy -

Reference:

https://docs.microsoft.com/en-us/azure/devops/repos/tfvc/add-check-policies https://azuredevopslabs.com/labs/vstsextend/sonarcloud/

Sylph Highly Voted 3 years, 5 months ago

Should be:

A build policy

A status policy

https://azuredevopslabs.com/labs/vstsextend/sonarcloud/

https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops#build-validation

upvoted 115 times

ahaz 3 years, 3 months ago

I agree

upvoted 2 times

rdemontis 2 years, 5 months ago
thanks for sharing the articles
upvoted 1 times

noussa 3 years, 4 months ago
I agree, I checked directly on Azure DevOps since I use it at work and as u said:
A build policy
A status policy
upvoted 9 times

Optimist_Indian 2 years, 7 months ago
Got this question in Feb-2022 exam (scored 910+). This is correct answer.
upvoted 12 times

francis6170 Highly Voted 3 years, 2 months ago
Got this in the AZ-400 exam (June 2021).
upvoted 11 times

4bd3116 Most Recent 4 months, 2 weeks ago
To ensure that your pull requests meet the specified criteria in Azure Repos, you should configure the following policy types:

For the requirement that committed code must compile successfully, you should configure a build policy. This policy will enforce that all code submitted in pull requests is built and passes all the configured tests before it can be merged.
For the requirement that pull requests must have a Quality Gate status of Passed in SonarCloud, you should configure a status policy. This policy will check the integration with SonarCloud to ensure that the code quality meets the defined standards before allowing the merge.
upvoted 1 times

Kalaisuran 5 months, 3 weeks ago
build policy
status policy

check policy are available only for TFVersion control
https://learn.microsoft.com/en-us/azure/devops/repos/tfvc/add-check-policies?view=azure-devops
upvoted 1 times

ozbonny 6 months, 3 weeks ago
A build policy
A status policy
upvoted 1 times

Hillah 8 months ago
build policy
status policy
upvoted 1 times

vsvaid 8 months, 4 weeks ago
Build Policy
Status Policy
upvoted 1 times

varinder82 9 months, 3 weeks ago
Final answer after reading all the commnts

1. build policy
2. status policy
upvoted 2 times

DGladiator 1 year, 3 months ago
Action 1: Committed code must compile successfully

Policy: Build policy

A build policy is used to ensure that any changes made to the code can be successfully built. This means that before changes can be merged, the code must compile successfully, which is the requirement you're trying to enforce. By using a build policy, you can ensure that every pull request

builds successfully before it's merged into the main branch.

Action 2: Pull requests must have a Quality Gate status of Passed in SonarCloud

Policy: Status policy

A status policy requires that an external service posts a status to the pull request. In this case, the external service would be SonarCloud. SonarCloud can analyze the code and check whether it meets the defined quality standards (Quality Gates). If it does, SonarCloud can then post a Passed status to the pull request. The status policy will then check this status before allowing the pull request to be merged.

Check-in policy is a term associated with TFVC (Team Foundation Version Control), not Git, hence it is not applicable here.
upvoted 6 times

RonZhong 1 year, 5 months ago
Status policy for SonarCloud
=> https://community.sonarsource.com/t/azure-devops-pull-request-quality-gate-status-check/33957/2
upvoted 1 times

RonZhong 1 year, 5 months ago
[X] Check-in policy is made for TFVC

https://learn.microsoft.com/en-us/azure/devops/repos/tfvc/add-check-policies?view=azure-devops
upvoted 1 times

Rams_84zO6n 1 year, 6 months ago
build, status
Successful last build, code analysis and work item association can be verified before every code commit in check-in policy. But this question is about PR request and not individual check-ins.
upvoted 1 times

syu31svc 2 years, 1 month ago
https://azuredevopslabs.com/labs/vstsextend/sonarcloud/

Committed code must compile successfully ---> Build policy
Pull requests must pass ---> Status Policy
upvoted 3 times

tjeerd 2 years, 1 month ago
On exam 20220727. Answer is:
Build policy
Status policy
upvoted 4 times

gs12345 2 years, 8 months ago
As per "Administrators of Team Foundation version control can add check-in policy.."
So Microsoft docs clearly mentions Check-in policy is for TFVC not Git, for git it is build policy.
answer is build and status policy as
upvoted 4 times

malikimran21 2 years, 9 months ago
this came in today exam Az-400 (Dec 2021)
upvoted 2 times

celciuz 3 years ago
This question came out, August 2021
upvoted 4 times

Question #27 *Topic 7*

You use a Git repository in Azure Repos to manage the source code of a web application. Developers commit changes directly to the default branch.

You need to implement a change management procedure that meets the following requirements:

- The default branch must be protected, and new changes must be built in the feature branches first.
- Changes must be reviewed and approved by at least one release manager before each merge.
- Changes must be brought into the default branch by using pull requests.

What should you configure in Azure Repos?

A. branch policies of the default branch

B. Services in Project Settings

C. Deployment pools in Project Settings

D. branch security of the default branch

Suggested Answer: *A*

Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards.

Reference:

https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies

Community vote distribution

A (100%)

goatlord Highly Voted 3 years, 1 month ago

Yes Good Correct

upvoted 11 times

Kazillius Highly Voted 3 years, 2 months ago

Correct

upvoted 5 times

ozbonny Most Recent 6 months, 3 weeks ago

Selected Answer: A

A. branch policies of the default branch

upvoted 1 times

zellck 1 year, 3 months ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops&tabs=browser

Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards.

upvoted 3 times

zellck 1 year, 3 months ago

Gotten this in Jun 2023 exam.

upvoted 1 times

AlexeyG 1 year, 6 months ago

got this in 02 March 2023 exams. scored 870 marks.

upvoted 3 times

syu31svc 2 years, 1 month ago

Selected Answer: A

A is correct as supported by given link

upvoted 1 times

kennynelcon 2 years, 2 months ago

Selected Answer: A

Correct, we can call this Master Branch ?

upvoted 2 times

Eltooth 2 years, 4 months ago

Selected Answer: A

A is correct answer.

upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: A

correct

upvoted 1 times

PlumpyTumbler 2 years, 7 months ago

Selected Answer: A

Branch policies

upvoted 1 times

Question #28 *Topic 7*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company uses Azure DevOps to manage the build and release processes for applications.
You use a Git repository for applications source control.
You need to implement a pull request strategy that reduces the history volume in the master branch.
Solution: You implement a pull request strategy that uses fast-forward merges.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
No fast-forward merge - This option merges the commit history of the source branch when the pull request closes and creates a merge commit in the target branch.
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies

Community vote distribution
B (100%)

fallenDaffy Highly Voted 4 years ago
Should be No. Squash merge - creates a linear history with a single commit in the target branch with the changes from the source branch.
upvoted 63 times

JimmyC Highly Voted 3 years, 4 months ago
I would argue that this answer is correct (keep in mind that these yes/no questions can have more than one Yes answer). Squash merge is also correct. However fast-forward merging does reduce the main branch history size, by not adding the merge itself into the history. Squash merging is a much better answer, but as the question is written, this answer is 100% correct.
upvoted 18 times

kennynelcon 2 years, 2 months ago
--ff merges the commit history of the source branch when the pull request closes and creates a merge commitin the target branch, and that is not in line with the question.
So maybe we can say it is wrong ?
upvoted 1 times

GPRai Most Recent 2 months, 3 weeks ago
Selected Answer: B
It should be Squash Merge
upvoted 1 times

ozbonny 6 months, 3 weeks ago
Selected Answer: B
Should be B. No
upvoted 1 times

ServerBrain 8 months, 2 weeks ago
Selected Answer: B
Question: 'a pull request strategy that reduces the history volume'
Best Answer: Squash merge..
upvoted 1 times

vsvaid 8 months, 4 weeks ago
Selected Answer: B
No for me

upvoted 1 times

yana_b 10 months, 3 weeks ago

Selected Answer: B

The proper solution is squash merge -> see link
https://learn.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops&tabs=browser

Basic merge (no fast-forward) creates a merge commit in the target whose parents are the target and source branches.

Squash merge creates a linear history with a single commit in the target branch with the changes from the source branch. Learn more about squash merging and how it affects branch history.

Rebase and fast-forward creates a linear history by replaying source commits onto the target branch with no merge commit.

Rebase with merge commit replays the source commits onto the target and also creates a merge commit.

upvoted 1 times

xRiot007 1 year, 1 month ago

We want to reduce the history volume, so SQUASH merge, not rebase. Also, in real life project, please do not use rebase, you will screw the history and nobody will understand anything anymore. At most you should use squash to condense things, but that's about it.

upvoted 1 times

MohmmadFayez 2 years, 1 month ago

There is No "Fast Forward merge" on azure repo
Azure repo has 4 merge option : 1) Basic (no fast forward) 2Squatch 3) rebase with fast forward 4) rebase with merge commit As i think the correct options which meet the rquirment here is - sqatch And - rebase with fast forward

upvoted 2 times

syu31svc 2 years, 1 month ago

Selected Answer: B

https://docs.microsoft.com/en-us/azure/devops/repos/git/merging-with-squash?view=azure-devops

"Squash merging is a merge option that allows you to condense the Git history"

Answer is No

upvoted 1 times

UnknowMan 2 years, 4 months ago

Selected Answer: B

Squash is a better solution

upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: B

answer is No, you need to use squash merge to condensate history

upvoted 1 times

cirojascr 2 years, 7 months ago

Selected Answer: B

fast forward takes all the commit messages

upvoted 1 times

Art3 2 years, 7 months ago

No is correct answer.

upvoted 2 times

Ycombo 2 years, 8 months ago

Selected Answer: B

It should be no. Squash merge is more appropriate.

upvoted 2 times

erickim007 3 years, 2 months ago

the answer should be no.

upvoted 1 times

monniq 3 years, 4 months ago

The provided answer contradicts with the explanation in MSDN. "Rebase and fast-forward - creates a linear history by replaying source commits onto the target branch with no merge commit."

I'd go with 'No'.

upvoted 2 times

Question #29 *Topic 7*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company uses Azure DevOps to manage the build and release processes for applications.
You use a Git repository for applications source control.
You need to implement a pull request strategy that reduces the history volume in the master branch.
Solution: You implement a pull request strategy that uses squash merges.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Instead use fast-forward merge.
Note:
Squash merge - Complete all pull requests with a squash merge, creating a single commit in the target branch with the changes from the source branch.
No fast-forward merge - This option merges the commit history of the source branch when the pull request closes and creates a merge commit in the target branch.
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies

Community vote distribution

A (100%)

fallenDaffy Highly Voted 4 years ago
Should be YES. Squash merge - creates a linear history with a single commit in the target branch with the changes from the source branch.
upvoted 69 times

Corona_Virus Highly Voted 4 years ago
Should be Yes
upvoted 16 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: A
Should be yes
upvoted 1 times

Hillah 8 months ago
Yes
https://itnext.io/git-merge-vs-rebase-vs-squash-8c3b6a2405e0
upvoted 1 times

vsvaid 8 months, 4 weeks ago
Selected Answer: A
Squash merge
upvoted 1 times

yana_b 10 months, 3 weeks ago
Squash to condense the history.
Rebase to override the history.
upvoted 1 times

zellck 1 year, 3 months ago
Gotten this in Jun 2023 exam.
upvoted 3 times

lucaseto 1 year, 8 months ago

Selected Answer: A

a squash merge adds all the file changes to a single new commit on the default branch

upvoted 2 times

icedog 1 year, 8 months ago

Selected Answer: A

A. Yes - 100%

Currently strategy I use at my work

upvoted 2 times

MohmmadFayez 2 years, 1 month ago

Azure repo has 4 merge option :

1) Basic (no fast forward)

2Squatch

3) rebase with fast forward

4) rebase with merge commit

As i think the correct options which meet the rquirment here is

- sqatch

And

- rebase with fast forward

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: A

Answer is Yes

https://docs.microsoft.com/en-us/azure/devops/repos/git/merging-with-squash?view=azure-devops

"Squash merging is a merge option that allows you to condense the Git history"

upvoted 1 times

adamsw 2 years, 2 months ago

Selected Answer: A

squash merges

upvoted 1 times

UnknowMan 2 years, 4 months ago

Selected Answer: A

Squash merge do the job

upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: A

answer is Yes. Squash merge are user just to condensate the history and all the topic commits in only one.

upvoted 1 times

Art3 2 years, 7 months ago

A, squash merge reduce commit history.

upvoted 1 times

Sara_Mo 2 years, 7 months ago

Selected Answer: A

Squash merge is the correct answer

upvoted 2 times

Surda 2 years, 8 months ago

Selected Answer: A

Squash merge is the correct answer

upvoted 1 times

Question #30 *Topic 7*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company uses Azure DevOps to manage the build and release processes for applications.
You use a Git repository for applications source control.
You need to implement a pull request strategy that reduces the history volume in the master branch.
Solution: You implement a pull request strategy that uses an explicit merge.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Instead use fast-forward merge.
Note:
No fast-forward merge - This option merges the commit history of the source branch when the pull request closes and creates a merge commit in the target branch.
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies

Community vote distribution
B (100%)

fallenDaffy Highly Voted 4 years ago
Instead, use Squash merge - creates a linear history with a single commit in the target branch with the changes from the source branch.
upvoted 21 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: B
Answer correct
upvoted 1 times

MohmmadFayez 2 years, 1 month ago
Explicit merge is relevant to "No fast forward merge"
So answer is no , becouse No fast forward will copy all commits history and add a commit messave to the target branch
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: B
Answer is No

Squash merging is a merge option that allows you to condense the Git history

From https://docs.microsoft.com/en-us/azure/devops/repos/git/merging-with-squash?view=azure-devops
upvoted 1 times

UnknowMan 2 years, 4 months ago
Selected Answer: B
Squash Merge
upvoted 1 times

rdemontis 2 years, 5 months ago
Selected Answer: B
correct answer but wrong explanation
upvoted 1 times

Kalaismile06 3 years, 3 months ago

The correct answer is No. This is yes or no type question and not the fill in the blank.

upvoted 3 times

roydeen 3 years, 9 months ago

Squash

upvoted 3 times

Question #31 *Topic 7*

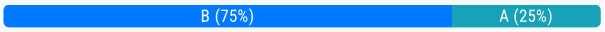
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company uses Azure DevOps to manage the build and release processes for applications.
You use a Git repository for applications source control.
You need to implement a pull request strategy that reduces the history volume in the master branch.
Solution: You implement a pull request strategy that uses a three-way merge.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Instead use fast-forward merge.
Note:
No fast-forward merge - This option merges the commit history of the source branch when the pull request closes and creates a merge commit in the target branch.
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies

Community vote distribution



fallenDaffy Highly Voted 4 years ago
Use Squash merge - creates a linear history with a single commit in the target branch with the changes from the source branch.
upvoted 22 times

truonghieu11111 3 years, 11 months ago
So what about your answer??
upvoted 1 times

ulhcx 3 years, 8 months ago
B - No
upvoted 3 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: B
correct no
upvoted 1 times

Sam90765 1 year, 8 months ago
Selected Answer: A
3 way merge = squash merge
upvoted 2 times

syu31svc 2 years, 1 month ago
Selected Answer: B
Answer is No

Squash merging is a merge option that allows you to condense the Git history

From https://docs.microsoft.com/en-us/azure/devops/repos/git/merging-with-squash?view=azure-devops
upvoted 2 times

UnknowMan 2 years, 4 months ago
Selected Answer: B

Squash merge do the job

upvoted 2 times

rdemontis 2 years, 5 months ago

Selected Answer: B

correct answer but wrong explanation

upvoted 1 times

leonelferrari 3 years, 3 months ago

use squash merge

upvoted 3 times

Hooters 3 years, 10 months ago

Its B - No

upvoted 2 times

Question #32 *Topic 7*

You need to recommend a Docker container build strategy that meets the following requirements:
➪ Minimizes image sizes
➪ Minimizes the security surface area of the final image
What should you include in the recommendation?

A. multi-stage builds

B. PowerShell Desired State Configuration (DSC)

C. Docker Swarm

D. single-stage builds

Suggested Answer: *A*
Multi-stage builds are a new feature requiring Docker 17.05 or higher on the daemon and client. Multistage builds are useful to anyone who has struggled to optimize Dockerfiles while keeping them easy to read and maintain.
Incorrect Answers:
C: A swarm consists of multiple Docker hosts which run in swarm mode and act as managers (to manage membership and delegation) and workers (which run swarm services).
Reference:
https://docs.docker.com/develop/develop-images/multistage-build/

Community vote distribution
A (100%)

msalvatori Highly Voted 4 years, 2 months ago
Correct - Verified
https://docs.docker.com/develop/develop-images/multistage-build/
upvoted 34 times

awron_durat Highly Voted 2 years, 7 months ago
Selected Answer: A
Multi-stage allows you to build and create in one container and grab just the compiled code to put in another. PowerShell DSC is for VM's and Docker Swarm is an Orchestration tool. Single-stage creates bigger builds.
upvoted 9 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: A
A. multi-stage builds
upvoted 1 times

yana_b 1 year, 1 month ago
Selected Answer: A
Muli-stage builds
upvoted 1 times

AlexeyG 1 year, 6 months ago
got this in 02 March 2023 exams. scored 870 marks.
upvoted 5 times

elequiel 1 year, 9 months ago
Selected Answer: A
Correct
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: A
B and C are out

Between A and D, A is the answer

"Minimizes the security surface area" so multi-stage build

upvoted 1 times

UnknowMan 2 years, 4 months ago

Correct

upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: A

correct

upvoted 1 times

jojom19980 3 years, 2 months ago

Multi-stage builds - Correct

upvoted 3 times

Question #33 *Topic 7*

You plan to create an image that will contain a .NET Core application.

You have a Dockerfile file that contains the following code. (Line numbers are included for reference only.)

```
01 FROM microsoft/dotnet: 3.1-sdk
02 COPY . /
03 RUN dotnet publish -c Release -o out
04 FROM microsoft/dotnet: 3.1-sdk
05 COPY --from=0 /out /
06 WORKDIR /
07 ENTRYPOINT [“dotnet”, “app1.dll”]
```

You need to ensure that the image is as small as possible when the image is built.

Which line should you modify in the file?

A. 1

B. 3

C. 4

D. 7

Suggested Answer: *A*

Multi-stage builds (in Docker 17.05 or higher) allow you to drastically reduce the size of your final image, without struggling to reduce the number of intermediate layers and files.

With multi-stage builds, you use multiple FROM statements in your Dockerfile. Each FROM instruction can use a different base, and each of them begins a new stage of the build. You can selectively copy artifacts from one stage to another, leaving behind everything you don't want in the final image.

Reference:

https://docs.docker.com/develop/develop-images/multistage-build/#use-multi-stage-builds

Community vote distribution

C (100%)

artisticcheese Highly Voted 4 years, 9 months ago

Correct answer is 4. Final image shall not be sdk but runtime image

upvoted 92 times

coma74 Highly Voted 4 years, 7 months ago

I agree correct answer is 4 because the production runtime doesn't include a sdk.

upvoted 16 times

4bd3116 Most Recent 4 months, 2 weeks ago

Selected Answer: C

line 04, change from using the SDK image to using a runtime image.

upvoted 1 times

ozbonny 6 months, 3 weeks ago

Selected Answer: C

Line 4 wrong

upvoted 1 times

Hillah 8 months ago

line 4

upvoted 1 times

vsvaid 8 months, 4 weeks ago

Selected Answer: C

Line 4

upvoted 1 times

yana_b 12 months ago

Selected Answer: C

This question is the same as question 25

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: C

Why do you need sdk twice?

Answer is C

upvoted 3 times

UnknowMan 2 years, 4 months ago

Selected Answer: C

Use a runtime image not a Sdk image to run the app

upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: C

correct answer is C. You don't need to use the SDK to run the application. You only need the runtime.

upvoted 2 times

lugospod 2 years, 7 months ago

Got this January 2022.

upvoted 4 times

cirojascr 2 years, 7 months ago

Selected Answer: C

Correct is line 4, should be taken the runtime environment image

upvoted 1 times

Sara_Mo 2 years, 7 months ago

Selected Answer: C

Correct answer is line 4. Final image shall not be sdk but runtime image

upvoted 1 times

rliberoff 2 years, 8 months ago

Selected Answer: C

It does not make sense to remove the SDK!!! How do you build then?
Come on @ExamTopics, it is obvious that the correct answer is C, line 04!
FIX THIS!

upvoted 1 times

arpi79 2 years, 9 months ago

Selected Answer: C

Correct answer is line 4. Final image shall not be sdk but runtime image

upvoted 1 times

AndyPix 2 years, 9 months ago

Selected Answer: C

Must use runtime, not sdk at line 4

upvoted 1 times

Keem 2 years, 11 months ago

The end result is the same tiny production image as before, with a significant reduction in complexity. You don't need to create any intermediate images and you don't need to extract any artifacts to your local system at all.

How does it work? The second FROM instruction starts a new build stage with the alpine:latest image as its base. The COPY --from=0 line copies just the built artifact from the previous stage into this new stage. The Go SDK and any intermediate artifacts are left behind, and not saved in the final image.

upvoted 2 times

Question #34 *Topic 7*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has a project in Azure DevOps for a new web application.
You need to ensure that when code is checked in, a build runs automatically.
Solution: From the Triggers tab of the build pipeline, you select Batch changes while a build is in progress.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Instead, In Visual Designer you enable continuous integration (CI) by:
1. Select the Triggers tab.
2. Enable Continuous integration.

Note: Batch changes -
Select this check box if you have many team members uploading changes often and you want to reduce the number of builds you are running. If you select this option, when a build is running, the system waits until the build is completed and then queues another build of all changes that have not yet been built.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/get-started-designer

Community vote distribution
B (100%)

Beast_Hollow Highly Voted 3 years, 4 months ago
Correct answer
upvoted 13 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: B
Correct B. No
upvoted 1 times

vsvaid 8 months, 4 weeks ago
Selected Answer: B
Agree to answer
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: B
https://docs.microsoft.com/en-us/devops/develop/what-is-continuous-integration

"Continuous integration (CI) is the process of automatically building and testing code every time a team member commits code changes to version control."

Answer is No
upvoted 1 times

UnknowMan 2 years, 4 months ago
Correct
upvoted 1 times

rdemontis 2 years, 5 months ago

Selected Answer: B

correct

upvoted 1 times

lugospod 2 years, 7 months ago

Got this January 2022.

upvoted 2 times

ScreamingHand 3 years, 1 month ago

Answer is correct: https://azuredevopslabs.com/labs/azuredevops/continuousintegration/

upvoted 3 times

Question #35 *Topic 7*

HOTSPOT -

You need to deploy Azure Kubernetes Service (AKS) to host an application. The solution must meet the following requirements:

➪ Containers must only be published internally.

➪ AKS clusters must be able to create and manage containers in Azure.

What should you use for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Containers must only be published internally:	Azure Container Instances Azure Container Registry Dockerfile
AKS clusters must be able to create and manage containers in Azure:	An Azure Active Directory (Azure AD) group An Azure Automation account An Azure service principal

Suggested Answer:

Answer Area

Containers must only be published internally:	Azure Container Instances Azure Container Registry Dockerfile
AKS clusters must be able to create and manage containers in Azure:	An Azure Active Directory (Azure AD) group An Azure Automation account An Azure service principal

Box 1: Azure Container Registry -

Azure services like Azure Container Registry (ACR) and Azure Container Instances (ACI) can be used and connected from independent container orchestrators like kubernetes (k8s). You can set up a custom ACR and connect it to an existing k8s cluster to ensure images will be pulled from the private container registry instead of the public docker hub.

Box 2: An Azure service principal

When you're using Azure Container Registry (ACR) with Azure Kubernetes Service (AKS), an authentication mechanism needs to be established. You can set up

AKS and ACR integration during the initial creation of your AKS cluster. To allow an AKS cluster to interact with ACR, an Azure Active Directory service principal is used.

Reference:

https://thorsten-hans.com/how-to-use-private-azure-container-registry-with-kubernetes https://docs.microsoft.com/en-us/azure/aks/cluster-container-registry-integration

nvnrao57 Highly Voted 3 years, 4 months ago

Given Ans is correct

upvoted 32 times

ougullamaija Highly Voted 2 years, 5 months ago

Correttamundo nella della mundo.

I am a huge fan of Docker, so obviously I can say with 100% certainty, that this is an absolutely marvellously correctamundo answer :)

upvoted 13 times

vsvaid Most Recent 8 months, 4 weeks ago

Agree with answer
upvoted 1 times

kmaneith 1 year, 10 months ago
is it "publish container image" ?
upvoted 1 times

vsvaid 8 months, 2 weeks ago
I was alos thinking about that. However publishing docker images means pushing it to registry so answer is correct.
https://docs.github.com/en/actions/publishing-packages/publishing-docker-images
upvoted 1 times

syu31svc 2 years, 1 month ago
https://docs.microsoft.com/en-us/azure/container-registry/authenticate-kubernetes-options

"AKS cluster AKS service principal Enable the AKS service principal with permissions to a target Azure container registry."

Answer is correct
upvoted 4 times

rdemontis 2 years, 5 months ago
correct answer
upvoted 1 times

lugospod 2 years, 7 months ago
Got this January 2022.
upvoted 4 times

igorole 3 years, 3 months ago
Fyi: https://docs.microsoft.com/en-us/azure/container-registry/authenticate-kubernetes-options
upvoted 6 times

rdemontis 2 years, 5 months ago
thanks for sharing the article
upvoted 1 times

Question #36 *Topic 7*

You have 50 Node.js-based projects that you scan by using WhiteSource. Each project includes Package.json, Package-lock.json, and Npm-shrinkwrap.json files.
You need to minimize the number of libraries reports by WhiteSource to only the libraries that you explicitly reference.
What should you do?

A. Configure the File System Agent plug-in.

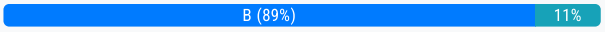
B. Add a devDependencies section to Package-lock.json.

C. Configure the Artifactory plug-in.

D. Delete Package-lock.json.

Suggested Answer: *B*
Separate Your Dependencies -
Within your package.json file be sure you split out your npm dependencies between devDependencies and (production) dependencies. The key part is that you must then make use of the --production flag when installing the npm packages. The --production flag will exclude all packages defined in the devDependencies section.
Reference:
https://blogs.msdn.microsoft.com/visualstudioalmrangers/2017/06/08/manage-your-open-source-usage-and-security-as-reported-by-your-cicd-pipeline/

Community vote distribution



klopper Highly Voted 4 years, 4 months ago
Is it a typo? There is no devDependencies in the package-lock.json.
The given comment refers to the devDependencies section in package.json
upvoted 26 times

chandru1dev 3 years, 1 month ago
It's a typo. In the comments, it's mentioned correctly
upvoted 3 times

Radul85 1 year, 7 months ago
Correttamundo !
upvoted 1 times

somedude Highly Voted 4 years, 3 months ago
Yeah, probably a typo. Here's a link to article describing similar scenario with WhiteSource:
https://docs.microsoft.com/en-us/archive/blogs/visualstudioalmrangers/manage-your-open-source-usage-and-security-as-reported-by-your-cicd-pipeline
upvoted 7 times

jasifu3 2 years, 6 months ago
according to your link, "whitesource will soon release an npm plugin" for this. The plugin is now released, so I would not be surprised if the question has been updated with the plugin as the correct answer.
upvoted 1 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: B
B. Add a devDependencies section to Package-lock.json.
upvoted 1 times

ObiWan500 10 months, 1 week ago
Selected Answer: A
Correct answer is A, not B

The File System Agent plug-in is a WhiteSource tool that scans the files and folders of your projects and reports the libraries and licenses that are detected. You can configure the File System Agent plug-in to scan only the Package.json files of your Node.js projects, and ignore the

Package-lock.json and Npm-shrinkwrap.json files. This way, you will minimize the number of libraries reported by WhiteSource to only the libraries that you explicitly reference in the Package.json files.

B. Adding a devDependencies section to Package-lock.json will not work, because the Package-lock.json file is automatically generated by npm and should not be manually edited. The devDependencies section in Package-lock.json reflects the devDependencies from the Package.json file of the dependency, not the project.

Source: Bing AI :)
upvoted 1 times

Fal991l 1 year, 5 months ago
GPT: Adding a devDependencies section to the package.json file in order to run npm install --omit-dev is a valid approach for reducing the size of the installed packages and the time it takes to install them, but it is not the correct solution for minimizing the number of libraries reports by WhiteSource to only the libraries that you explicitly reference.

The devDependencies section in package.json is used to specify the packages that are only required for development and testing, and not for the production use of the project. By default, the npm install command installs all dependencies, including those specified in devDependencies.

However, by running npm install --omit-dev, you can exclude the packages listed in devDependencies from being installed. This can help reduce the size of the installed packages and the time it takes to install them, especially in production environments where only the packages needed for runtime are required.
upvoted 1 times

Fal991l 1 year, 5 months ago
But to minimize the number of libraries reports by WhiteSource to only the libraries that you explicitly reference, you need to delete the npm-shrinkwrap.json and package-lock.json files and only keep the package.json file in each of the 50 Node.js-based projects.
upvoted 1 times

smariussorin 1 year, 7 months ago
Selected Answer: B
Typo, it should be:
" Add a devDependencies section to Package.json." in order to run npm install --omit-dev
upvoted 1 times

Schtrudl 2 years ago
Selected Answer: B
Correct Answer is B
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: B
https://docs.microsoft.com/en-us/archive/blogs/visualstudioalmrangers/manage-your-open-source-usage-and-security-as-reported-by-your-cicd-pipeline:

"Within your package.json file be sure you split out your npm dependencies between devDependencies and (production) dependencies"

Answer is B (though like what others before me have pointed out, it's a typo; package.json and not package lock)
upvoted 3 times

UnknowMan 2 years, 4 months ago
B. Add a devDependencies section to Package.json. (Not Package-lock.json)
upvoted 2 times

rdemontis 2 years, 5 months ago
Selected Answer: B
correct answer but the change has to be made to package.json file
upvoted 2 times

fragtom 3 years, 5 months ago
Info for related url https://docs.microsoft.com/en-us/azure/devops/migrate/security-validation-cicd-pipeline?view=azure-devops
upvoted 2 times

DeepMoon 3 years, 6 months ago

Why do we need lock files?

Lock files are intended to pin down, or lock, all versions for the entire dependency tree at the time that the lock file is created. Why is it important to use a package lock file and lock package versions?

Without a package lock file, a package manager such as Yarn or npm will resolve the the most current version of a package in real-time during the dependencies install of a package, rather than the version that was originally intended for the specific package

upvoted 3 times

27close 3 years, 10 months ago

answer B-confirm

upvoted 2 times

glaedr 4 years, 1 month ago

Answer correct solving the typo error. It should be package.json instead of package-lock.json
https://docs.npmjs.com/specifying-dependencies-and-devdependencies-in-a-package-json-file

upvoted 4 times

pnkumar 4 years, 3 months ago

According to this https://docs.microsoft.com/en-us/azure/devops/pipelines/ecosystems/javascript?view=azure-devops&tabs=code answer should be package.json

upvoted 5 times

Question #37 *Topic 7*

Your company deploys applications in Docker containers.
You want to detect known exploits in the Docker images used to provision the Docker containers.
You need to integrate image scanning into the application lifecycle. The solution must expose the exploits as early as possible during the application lifecycle.
What should you configure?

A. a task executed in the continuous integration pipeline and a scheduled task that analyzes the image registry

B. manual tasks performed during the planning phase and the deployment phase

C. a task executed in the continuous deployment pipeline and a scheduled task against a running production container

D. a task executed in the continuous integration pipeline and a scheduled task that analyzes the production container

Suggested Answer: *A*
You can use the Docker task to sign into ACR and then use a subsequent script to pull an image and scan the container image for vulnerabilities.
Use the docker task in a build or release pipeline. This task can be used with Docker or Azure Container registry.
Incorrect Answers:
C: We should not wait until deployment. We want to detect the exploits as early as possible.
D: We should wait until the image is in the product container. We want to detect the exploits as early as possible.
Reference:
https://docs.microsoft.com/en-us/azure/devops/articles/security-validation-cicd-pipeline?view=vsts

Community vote distribution
A (100%)

TechieBloke Highly Voted 4 years, 1 month ago
No way you should do manual task. And the requirement states "as early as possible" so image registry is the earliest option from the other 3 what left.
Answer is correct.
upvoted 20 times

Radul85 1 year, 7 months ago
Correttamundo !
upvoted 1 times

joseluismantilla Highly Voted 4 years, 3 months ago
This is a new feature release in March, https://docs.microsoft.com/en-us/azure/security-center/azure-container-registry-integration

Now, in your pipeline, trivy/aqua would be the task.
upvoted 8 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: A
A. a task executed in the continuous integration pipeline and a scheduled task that analyzes the image registry
upvoted 2 times

Deequation 1 year, 10 months ago
Why is CI a better place to scan, than in CD? Sure, if it's a known issue, you catch it already in CI step. But what if you run your CI, nothing is found. Then months later you want to deploy your build, or even revert to an old one. Now you are just going to run your CD, but in the meantime, issues could have been found. This will not be detected by running the scan exclusively in build.
upvoted 2 times

syu31svc 2 years, 1 month ago
Selected Answer: A
https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-cicd

"To set up the scanner, you'll need to enable Microsoft Defender for container registries and the CI/CD integration"

Answer is A

upvoted 1 times

Eltooth 2 years, 4 months ago

Selected Answer: A

A is correct answer.

upvoted 1 times

UnknowMan 2 years, 4 months ago

Never do in OnProd env and no manual, so Answer is correct. => image registry

upvoted 2 times

rdemontis 2 years, 5 months ago

Selected Answer: A

for the correct answer is A. CI and ACR are the places to scan for security issues as early as possible

upvoted 1 times

jojom19980 3 years, 3 months ago

The answer is looking correct :https://docs.microsoft.com/en-us/azure/security-center/defender-for-container-registries-cicd

upvoted 5 times

Duleep 4 years, 2 months ago

why we need to analyze image registry?, it would be faster analyze only required images

upvoted 1 times

cucuff 4 years, 1 month ago

I have the same doubt, but the others answers are a big NO, so i suppose A is the correct answer

upvoted 4 times

whoisthis 3 years, 8 months ago

You need to scan image registry because vulnerabilities could be found even after you successfully scan it during your CI when the vulnerabilities database does not yet contain the CVE

upvoted 3 times

combo_breaker 3 years, 6 months ago

Faster.. yes. But since analyzing the image registry will be a scheduled task (not one that is ran while you are running your CI/CD pipeline) it hopefully shouldn't matter how long it takes. Schedule it for Saturday-Sunday morning if time is an issue for ya.

upvoted 3 times

Ivjo 4 years, 2 months ago

Answer looks right, but it is not scheduled. It's done on the every push stage, no ?

upvoted 3 times

Yong2020 3 years, 10 months ago

There might be images not pushed through code, e.g. manually uploaded images, they need to be scanned to be secured. So a scheduled scan is also required just to cover 100% cases.

upvoted 3 times

Question #38 *Topic 7*

Your company has a hybrid cloud between Azure and Azure Stack.
The company uses Azure DevOps for its full CI/CD pipelines. Some applications are built by using Erlang and Hack.
You need to ensure that Erlang and Hack are supported as part of the build strategy across the hybrid cloud. The solution must minimize management overhead.
What should you use to execute the build pipeline?

A. a Microsoft-hosted agent

B. Azure DevOps self-hosted agents on Azure DevTest Labs virtual machines.

C. Azure DevOps self-hosted agents on Hyper-V virtual machines

D. Azure DevOps self-hosted agents on virtual machines that run on Azure Stack

Suggested Answer: *D*
Azure Stack offers virtual machines (VMs) as one type of an on-demand, scalable computing resource. You can choose a VM when you need more control over the computing environment.
Reference:
https://docs.microsoft.com/en-us/azure/azure-stack/user/azure-stack-compute-overview

Community vote distribution

D (100%)

AzureGurl Highly Voted 4 years, 1 month ago
D is the correct answer.
upvoted 24 times

skySand Highly Voted 3 years, 7 months ago
D is the correct answer.
As the question says that some applications are build using Erlang and Hack (which could be something dependent component) that is needed for the build to execute.. for which self-hosted agent on VM is needed as the build execution will happen on the build server
upvoted 7 times

ozbonny Most Recent 6 months, 3 weeks ago
Selected Answer: D
D. Azure DevOps self-hosted agents on virtual machines that run on Azure Stack
upvoted 1 times

kinkekin 1 year, 8 months ago
Selected Answer: D
Correct Answer.
upvoted 2 times

syu31svc 2 years, 1 month ago
Selected Answer: D
https://azure.microsoft.com/en-us/products/azure-stack/#overview

"Build, deploy, and run hybrid and edge computing apps"

https://docs.microsoft.com/en-us/azure-stack/user/azure-stack-compute-overview?view=azs-2102

"You can use Azure Stack Hub VMs in several ways. For example:

Development and test: Azure Stack Hub VMs enable you to create a computer with a specific configuration required to code and test an application.

Applications in the cloud: Because demand for your application can fluctuate, it might make economic sense to run it on a VM in Azure Stack Hub. You pay for extra VMs when you need them and shut them down when you don't."

Answer is D

upvoted 1 times

Eltooth 2 years, 4 months ago

Selected Answer: D

D is correct answer.

upvoted 2 times

lugospod 2 years, 7 months ago

Got this January 2022. Went with D. Got 100% on that part.

upvoted 5 times

celciuz 3 years ago

This question came out, August 2021

upvoted 4 times

vglearn 3 years, 7 months ago

Answer is correct

upvoted 1 times

aftab7500 3 years, 10 months ago

Azure DevTest Labs is used for only testing purpose.

upvoted 5 times

rdemontis 2 years, 5 months ago

thanks for explanation

upvoted 1 times

JohnD2020 4 years, 5 months ago

Should be answer B as Azure Stack requires more management than DevTest Labs.

upvoted 1 times

hubeau 4 years, 5 months ago

And also "across the hybrid cloud"

upvoted 9 times

hubeau 4 years, 5 months ago

It should be work in production environment so D is good answer

upvoted 19 times

d0bermannn 2 years, 11 months ago

yes, if az stack inplemented already on-prem)

upvoted 2 times

Question #39 *Topic 7*

Your company has an Azure DevOps project,
The source code for the project is stored in an on-premises repository and uses on an on-premises build server.
You plan to use Azure DevOps to control the build process on the build server by using a self-hosted agent.
You need to implement the self-hosted agent.
You download and install the agent on the build server.
Which two actions should you perform next? Each correct answer presents part of the solution.

A. From Azure, create a shared access signature (SAS).

B. From the build server, create a certificate, and then upload the certificate to Azure Storage.

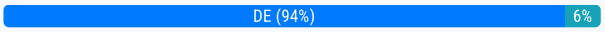
C. From the build server, create a certificate, and then upload the certificate to Azure Key Vault.

D. From DevOps, create a personal access token (PAT).

E. From the build server, run config.cmd.

Suggested Answer: *BE*
B: Make sure you install your self-signed ssl server certificate into the OS certificate store.
E: When you have a self-signed SSL certificate for your on-premises TFS server, make sure to configure the Git we shipped to allow that self-signed SSL certificate.
Enable git to use SChannel during configure with 2.129.0 or higher version agent Pass --gituseschannel during agent configuration
./config.cmd --gituseschannel
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/certificate

Community vote distribution



eray95 Highly Voted 3 years, 10 months ago
For the successful agent installing we need the PAT, question is not clear but we create PAT firstly, after that run config.cmd for agent installation
Could be D and E??
upvoted 78 times

shankatna 3 years, 5 months ago
I will go with options D and E, I tested self hosted agent by creating an VM, after downloading the agent,. before executing config.sh we need to have PAT created from Azure DevOPS https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/v2-linux?view=azure-devops
upvoted 8 times

Hooters 3 years, 10 months ago
It should be D and E
upvoted 11 times

Dfg2001 3 years, 10 months ago
D and E is correct. See https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/v2-windows?view=azure-devops (Get PAT, run config)
upvoted 28 times

kumardeb Highly Voted 3 years, 10 months ago
D. From DevOps, create a personal access token (PAT).
E. From the build server, run config.cmd.
upvoted 18 times

GPRai Most Recent 2 months, 3 weeks ago
Selected Answer: DE
I have tested this solution. For sure it is D & E.
upvoted 1 times

FeriAZ 6 months ago
Selected Answer: DE
D. Personal Access Token (PAT): A PAT is the primary way for a self-hosted agent to authenticate with Azure DevOps Pipelines.

E. Run config.cmd:
This command is crucial for configuring the self-hosted agent. It registers the agent with your Azure DevOps organization, establishing the connection and allowing the agent to communicate with Azure DevOps Pipelines.
upvoted 1 times

smariussorin 1 year, 7 months ago
Selected Answer: DE
When generating the config strict, you have the option to include your PAT automatically
upvoted 2 times

mrg998 1 year, 8 months ago
Selected Answer: DE
Anwser is D and E. Its literally written here - https://learn.microsoft.com/en-us/azure/devops/pipelines/agents/v2-windows?view=azure-devops
upvoted 2 times

syu31svc 2 years, 1 month ago
Selected Answer: DE
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/v2-windows?view=azure-devops

1) Authenticate with a personal access token (PAT)
2) run config.cmd

D and E are the answers
upvoted 5 times

Eltooth 2 years, 4 months ago
Selected Answer: DE
D & E are correct answers.
upvoted 3 times

demonite 2 years, 4 months ago
Selected Answer: DE
101% DE
upvoted 2 times

UnknowMan 2 years, 4 months ago
Selected Answer: DE
After agent is install, we need to execute PS C:\agent> .\config.cmd and we need a PAT
upvoted 3 times

rdemontis 2 years, 5 months ago
Selected Answer: DE
D and E are the correct answers.
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/v2-windows?view=azure-devops
upvoted 2 times

ougullamaija 2 years, 5 months ago
Selected Answer: BE
corect is this
upvoted 2 times

Art3 2 years, 7 months ago
DE are correct IMO.
upvoted 1 times

darsh19 2 years, 8 months ago
Selected Answer: DE
https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/v2-windows?view=azure-devops
upvoted 4 times

Sandosh_N2 2 years, 9 months ago
Selected Answer: DE
D & E
upvoted 4 times

ChauPhan 2 years, 10 months ago

We can use either HTTPS client/server side certificates or PAT to authenticate on-premise repo and build server. However, it does not make sense for uploading the certificate to Azure, the certificate should be on on-premise servers for authentication.

I go with D and E

upvoted 1 times

Minatodsenspei 3 years, 2 months ago

D and E definitely

upvoted 3 times

Question #40 *Topic 7*

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant.
You are configuring a build pipeline in Azure Pipelines that will include a task named Task1. Task1 will authenticate by using an Azure AD service principal.
Which three values should you configure for Task1? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. the tenant ID

B. the subscription ID

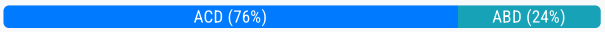
C. the client secret

D. the app ID

E. the object ID

Suggested Answer: *ABD*
Create an Azure Resource Manager service connection with an existing service principal
AB: Enter the information about your service principal into the Azure subscription dialog textboxes:
➪ Tenant ID
➪ Subscription ID
➪ Subscription name
➪ Service principal ID
Either the service principal client key or, if you have selected Certificate, enter the contents of both the certificate and private key sections of the *.pem file.
D: To deploy to a specific Azure resource, the task will need additional data about that resource.
If you're using the classic editor, select data you need. For example, the App service name.
If you're using YAML, then go to the resource in the Azure portal, and then copy the data into your code. For example, to deploy a web app, you would copy the name of the App Service into the WebAppName value.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/library/connect-to-azure

Community vote distribution



wblom Highly Voted 3 years, 10 months ago
Should be
A. the tenant ID
D. the app ID
C. the client secret
upvoted 87 times

kamyrkon 2 years, 6 months ago
Correct, in task1 we can use powershell for connection, so could use Tenant ID, App ID, secret
https://docs.microsoft.com/en-us/powershell/azure/authenticate-azureps?view=azps-7.3.0#sign-in-with-a-service-principal
upvoted 1 times

tom999 3 years, 7 months ago
From https://azuredevopslabs.com/labs/devopsserver/azureserviceprincipal/ (see also the screenshots there)
...
4. Run "az ad sp create-for-rbac --name ServicePrincipalName"
5. Azure will generate an appID, which is the Service principal client ID used by Azure DevOps Server. It will also generate a strong password, which is the Service principal key. The final value of interest is the tenant, which is the Tenant ID...
6. Execute "az account show"
7. The id is the Subscription ID you need to create the service connection. The name is the Subscription name you need.

>> I validated this approach .
>> Conclusion: The given answer ABD is correct.

It is a bit confusing because the fields in Azure Devops "Create service connection" have different names than in the CLI output. But there is no "client secret" and no "object id".
upvoted 26 times

monniq 3 years, 4 months ago
This answer is well supported, and most legit.
upvoted 5 times

kumardeb Highly Voted 3 years, 10 months ago
A. the tenant ID
C. the client secret
D. the app ID
upvoted 14 times

ieboaix Most Recent 1 year, 1 month ago
ABD verified
upvoted 2 times

yana_b 1 year, 1 month ago
Answer and its explanation are correct, as in Az DevOps we have to input the fileds listed in the explanation. However, the Service principal ID in Az Devops is actually the app ID used for creating the service rpincipal. So when you follow the steps from this link https://docs.microsoft.com/en-us/azure/devops/pipelines/library/connect-to-azure ti fill in the service principal ID you have to paste there the appID -> see Task 2, point 5 of this lab https://azuredevopslabs.com/labs/devopsserver/azureserviceprincipal/
upvoted 1 times

BuddhiK 1 year, 8 months ago
I think ABD is correct. If you deploy with SP it will not asked secret when deploying through Azure Pipelines. But if you are deploying through PowerShell you have define secret and app ID. So for this answer should be ABD.

Below are the steps for PS deployment:
1. Define tenant
2. Define Subscription
3. Provide App registration details .(APP ID and Password)
For Azure Pipeline
1. Tenant is already defined
2. APP ID or SPN
3. Subscription ID
upvoted 2 times

Atos 1 year, 12 months ago
The Azure Resource Manager service connection asks for the following config:

A. the tenant ID
B. the subscription ID
C. the client secret
D. the app ID

To test an azure service principal you will need

1. Service principal application ID.
2. Service principal key.
3. Your Azure AD tenant ID.

Therefore i'd be inclined to put:

A. the tenant ID
C. the client secret
D. the app ID
upvoted 3 times

giuliohome 2 years ago
Selected Answer: ACD

From https://docs.microsoft.com/en-us/learn/modules/authenticate-azure-deployment-pipeline-service-principals/6-exercise-authorize-service-principal-deployments?pivots=powershell#deploy-the-bicep-file-by-using-the-service-principal
...you'll simulate what a pipeline does to deploy ...
Use the service principal's application ID and key (so D and C) to get the credentials.
Then, to sign in by using the service principal's credentials, you are asked also the tenant id (A)
upvoted 2 times

syu31svc 2 years, 1 month ago

Selected Answer: ABD

https://docs.microsoft.com/en-us/azure/devops/pipelines/library/connect-to-azure?view=azure-devops

Enter the information about your service principal into the Azure subscription dialog textboxes:

Subscription ID

ABD is the answer
upvoted 1 times

syu31svc 2 years ago

Sorry after reviewing it should be ACD

https://docs.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals

"When you've completed the app registration, you've a globally unique instance of the app (the application object) which lives within your home tenant or directory. You also have a globally unique ID for your app (the app or client ID). In the portal, you can then add secrets or certificates and scopes to make your app work, customize the branding of your app in the sign-in dialog, and more."
upvoted 1 times

tjeerd 2 years, 1 month ago

Selected Answer: ACD

On exam 20220727. Question was phrased a little different there, with combinations of the different components.
upvoted 2 times

Manjubk 2 years, 1 month ago

Selected Answer: ABD

Go to Azure Devops-->Projects Settings-->Service Connection.
Then you will see the
➪ Tenant ID
➪ Subscription ID
➪ Subscription name
➪ Service principal ID
upvoted 2 times

Redimido 2 years, 2 months ago

Selected Answer: ABD

Having those, anyone can impersonate as your app.
upvoted 1 times

Eltooth 2 years, 4 months ago

Selected Answer: ACD

A C & D are correct answers.
upvoted 2 times

Lucario95 2 years, 4 months ago

Selected Answer: ACD

Should be A, C, D
upvoted 2 times

UnknowMan 2 years, 4 months ago

Selected Answer: ACD

Acd is the correct answer
upvoted 2 times

UnknowMan 2 years, 4 months ago

A. the tenant ID

C. the client secret

D. the app ID

upvoted 2 times

rdemontis 2 years, 5 months ago

Selected Answer: ABD

IMHO answer is correct. To allow a build pipeline task to authenticate to AAD with an existing Service Principal you have to follow the procedure "Create an Azure Resource Manager service connection with an existing service principal" in the documented below

https://docs.microsoft.com/en-us/azure/devops/pipelines/library/connect-to-azure?view=azure-devops#create-an-azure-resource-manager-service-connection-with-an-existing-service-principal

upvoted 1 times

STH 2 years, 6 months ago

Selected Answer: ACD

there is no ask for subscriptionID when using app credentials, but only tenant, client ID (ie. app ID) and client secret (ie. app secret)

upvoted 2 times

Question #41 *Topic 7*

DRAG DROP -

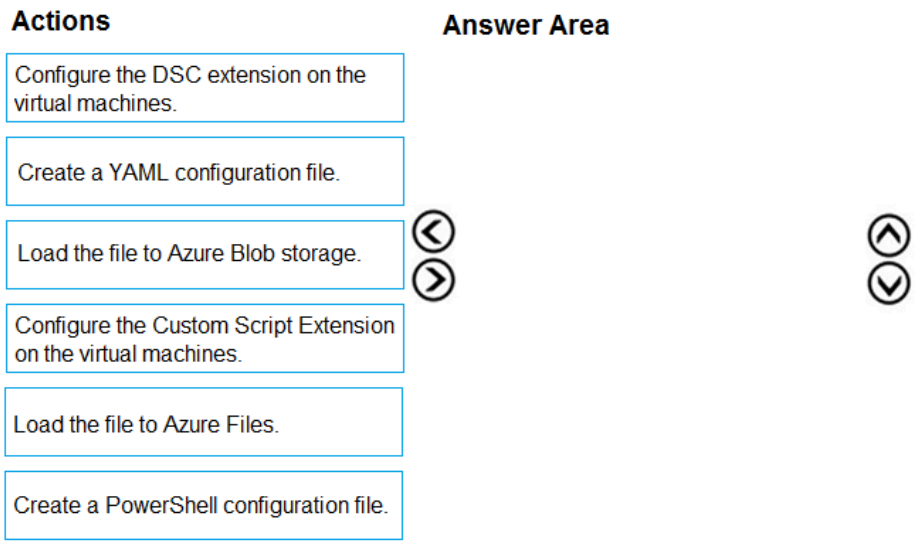
You are deploying a new application that uses Azure virtual machines.

You plan to use the Desired State Configuration (DSC) extension on the virtual machines.

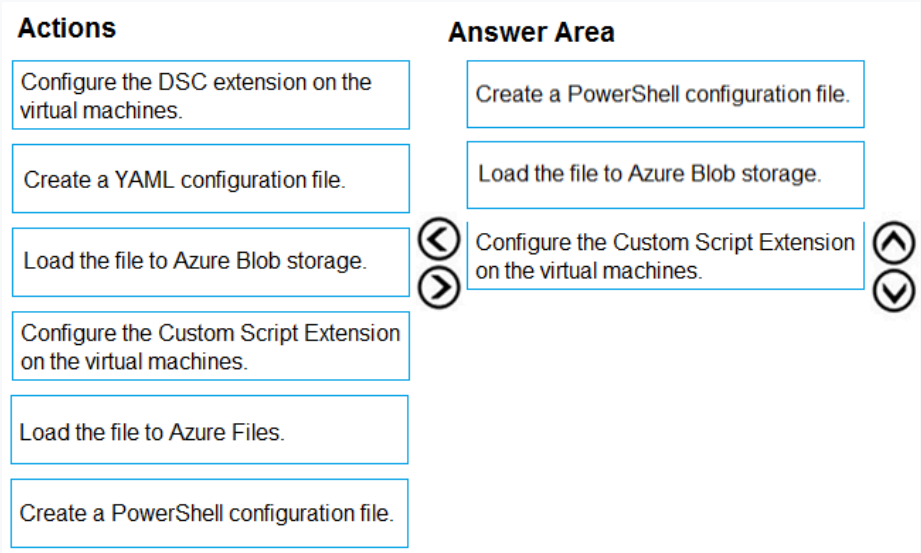
You need to ensure that the virtual machines always have the same Windows feature installed.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Suggested Answer:



Step 1: Create a PowerShell configuration file

You create a simple PowerShell DSC configuration file.

Step 2: Load the file to Azure Blob storage

Package and publish the module to a publically accessible blob container URL

Step 3: Configure the Custom Script Extension on the virtual machines.

The Custom Script Extension downloads and executes scripts on Azure virtual machines.

Reference:

https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/custom-script-windows

Tesshu Highly Voted 3 years, 5 months ago

I believe gicen answer is wrong, it should be:

1. Create a PowerShell configuration file
2. Load the file to Azure Blob storage
3. Configure the *DSC extension* on the virtual machines

https://docs.microsoft.com/en-us/azure/automation/automation-dsc-onboarding
upvoted 101 times

khengoolman 2 years, 10 months ago
Your link doesn't explain why Azure Blob is correct, this explains it a bit better: https://marckean.com/2018/06/28/azure-automation-dsc-config-example/
I agree with your answers
upvoted 5 times

rdemontis 2 years, 5 months ago
agree with you
upvoted 2 times

Kinon4 Highly Voted 3 years, 4 months ago
Question is asking you to use DSC, why would you use Custom Script Extension?
I believe answer is:

1. Create a Powershell configuration file
2. Load the file to Azure Blob storage
3. Configure the DSC extension on the virtual machines
upvoted 10 times

vsvaid Most Recent 8 months, 4 weeks ago
Create Powershell script
Load to storahe
Configure DSC
upvoted 1 times

dipti927 1 year, 3 months ago
To ensure that the virtual machines always have the same Windows feature installed using the Desired State Configuration (DSC) extension in Azure, you should perform the following actions in sequence:

Create a DSC configuration script: Write a DSC configuration script that includes the necessary steps to ensure the desired Windows feature is installed on the virtual machines. The configuration script defines the desired state of the system.

Upload the DSC configuration script to an accessible location: Store the DSC configuration script in a location that the virtual machines can access, such as Azure Storage, a version control repository, or a shared network location.

Configure the DSC extension on the virtual machines: Use the Azure portal, Azure PowerShell, Azure CLI, or Azure Resource Manager (ARM) templates to configure the DSC extension on the virtual machines. Specify the location of the DSC configuration script and any additional settings required for the extension.
upvoted 3 times

Fal991l 1 year, 5 months ago
Based on a discussion with GPT:
1. Create a YAML configuration file (B) that specifies the Windows feature to be installed.
2. Create a PowerShell configuration file (F) that references the YAML file and configures the DSC extension on the virtual machines.
3. Configure the DSC extension on the virtual machines (A) using the PowerShell configuration file.
upvoted 1 times

Fal991l 1 year, 5 months ago
Note that the YAML configuration file is needed to specify the Windows feature to be installed, and the PowerShell configuration file references the YAML file and configures the DSC extension on the virtual machines. The SAS token in blob storage is also needed to secure the YAML configuration file, but it is not one of the three actions required to ensure that the virtual machines always have the same Windows feature installed.
upvoted 1 times

syu31svc 2 years, 1 month ago
https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview

"The configuration data file is secured by an SAS token in blob storage"

1) Create a PowerShell configuration file
2) Load the file to Azure Blob storage
3) Configure the DSC extension on the virtual machines
upvoted 5 times

Eltooth 2 years, 4 months ago
Create PS
Load to Blob
Configure DSC
upvoted 2 times

UnknowMan 2 years, 4 months ago
"always have the same Windows feature installed." Mean DSC extension that manage drift
1. Create a PowerShell configuration file
2. Load the file to Azure Blob storage
3. Configure the *DSC extension* on the virtual machines
upvoted 3 times

jay158 2 years, 4 months ago
Please note the question says 'Azure virtual machines'
What if there are 1000 machine?
To stop the configuration from drifting we need automation account also.
In short Ans Should be
1. Create a PowerShell configuration file
2. Load the file to Azure Blob storage
3. Configure ARM Template -- to apply and configure DSC extensions + also create automation account
upvoted 2 times

lugospod 2 years, 7 months ago
Got this January 2022.
upvoted 5 times

andruhan 2 years, 9 months ago
I believe it should be Blob Storage, see:
https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview#dsc-extension-powershell-cmdlets

The following commands place the iisInstall.ps1 script on the specified VM. The commands also execute the configuration, and then report back on status.

```
$resourceGroup = 'dscVmDemo'
$vmName = 'myVM'
$storageName = 'demostorage'
#Publish the configuration script to user storage
Publish-AzVMDscConfiguration -ConfigurationPath .\iisInstall.ps1 -ResourceGroupName $resourceGroup -StorageAccountName $storageName -force
#Set the VM to run the DSC configuration
Set-AzVMDscExtension -Version '2.76' -ResourceGroupName $resourceGroup -VMName $vmName -ArchiveStorageAccountName $storageName -ArchiveBlobName 'iisInstall.ps1.zip' -AutoUpdate -ConfigurationName 'IISInstall'
```
upvoted 1 times

ChauPhan 2 years, 10 months ago
The questions are weird. We need to upload the DCS Config file to Azure Automation, compile it then add the Nodes that we need to configuration monitoring. I am not sure why we add it to Azure File or Blob
upvoted 3 times

Kolego 2 years, 11 months ago
I answered:
1. Create a Powershell configuration file
2. Load the file to AZURE FILES (!!!)
3. Configure the DSC extension on the virtual machine

I am not sure about the 2. There is a chance that both Blob and Files are correct.
Got 870pts
upvoted 3 times

mpknz 3 years, 2 months ago
Based on https://docs.microsoft.com/en-us/powershell/scripting/dsc/pull-server/pullserver?view=powershell-7.1 I think the answer may be to load the powershell config file onto a SMB share i.e. Azure Files not Blob storage and configure the DSC extension. I haven't seen any document suggesting a solution involving blob storage
upvoted 1 times

SACHMAM 3 years, 2 months ago
True question is saying DSC. we shouldn't be using CSE here
I feel right answer is

1. Create a Powershell configuration file
2. Load the file to Azure Blob storage
3. Configure the DSC extension on the virtual machine

Sachin Kadam
upvoted 5 times

sam441 3 years, 2 months ago
correct answer
upvoted 1 times

Question #42 *Topic 7*

You need to execute inline testing of an Azure DevOps pipeline that uses a Docker deployment model. The solution must prevent the results from being published to the pipeline.
What should you use for the inline testing?

A. a single stage Dockerfile

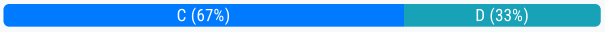
B. an Azure Kubernetes Service (AKS) pod

C. a multi-stage Dockerfile

D. a Docker Compose file

Suggested Answer: *D*
Use Docker when running integration tests with Azure Pipelines.
Reference:
https://crossprogramming.com/2019/12/27/use-docker-when-running-integration-tests-with-azure-pipelines.html

Community vote distribution



yhredil Highly Voted 3 years, 10 months ago
It should be C. a multi-stage Dockerfile
"Build and test with a multi-stage Dockerfile: build and tests execute inside the container using a multi-stage Docker file, as such test results are not published back to the pipeline."
https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/test/publish-test-results?view=azure-devops&tabs=trx%2Cyaml
upvoted 81 times

Tealon Highly Voted 3 years, 9 months ago
For Docker based apps there are many ways to build your application and run tests:

Build and test in a build pipeline: build and tests execute in the pipeline and test results are published using the Publish Test Results task.

Build and test with a multi-stage Dockerfile: build and tests execute inside the container using a multi-stage Docker file, as such test results are not published back to the pipeline.

Build, test, and publish results with a Dockerfile: build and tests execute inside the container and results are published back to the pipeline. See the example below.

--> So multi-stage docker file.

https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/test/publish-test-results?view=azure-devops&tabs=trx%2Cyaml
upvoted 12 times

rdemontis 2 years, 5 months ago
agree with you
upvoted 1 times

FeriAZ Most Recent 6 months ago
Selected Answer: C
Inline Testing Requirements:

The goal is to execute tests within the pipeline without impacting the final image or published test results.
We want to isolate the testing environment from the build process.

Separation of Concerns
No Test Result Publication
upvoted 1 times

vsvaid 8 months, 4 weeks ago

Selected Answer: C

Multi Stage Dockerfile. We can build and test in the pipeleine

upvoted 1 times

ObiWan500 10 months, 1 week ago

Selected Answer: D

To prevent the test results from being published to the pipeline, you can use the --exit-code-from option when running the docker-compose up command.

upvoted 1 times

yana_b 10 months, 4 weeks ago

Selected Answer: C

Build and test in a build pipeline: builds and tests execute in the pipeline and test results are published using the Publish Test Results task.
Build and test with a multi-stage Dockerfile: builds and tests execute inside the container using a multi-stage Docker file, as such test results are not published back to the pipeline.
Build, test, and publish results with a Dockerfile: builds and tests execute inside the container, and results are published back to the pipeline. See the example below.

https://learn.microsoft.com/en-us/azure/devops/pipelines/tasks/reference/publish-test-results-v2?view=azure-pipelines&viewFallbackFrom=azure-devops&tabs=trx%2Ctrxattachments%2Cyaml#docker

upvoted 1 times

Pamban 1 year, 2 months ago

Selected Answer: D

this question appeared on today's (20/06/23) exam.selected D. scored 955. should be correct! cheers

upvoted 3 times

rahul51it 1 year, 7 months ago

C. a multi-stage Dockerfile

upvoted 1 times

syu31svc 2 years, 1 month ago

Selected Answer: C

B and D are wrong for sure

Between A and C, C is the answer

Multi-stage builds are preferred

upvoted 1 times

Manjubk 2 years, 1 month ago

Selected Answer: C

Build and test in a build pipeline v/s
Build and test with a multi-stage Dockerfile: v/s
Build, test, and publish results with a Dockerfile:

So, Build and test with a multi-stage Dockerfile: satisfy this.

upvoted 1 times

UnknowMan 2 years, 4 months ago

Selected Answer: C

Multistage is right answer

upvoted 2 times

Whirly 2 years, 5 months ago

Exam Question April 1st 2022, went with Multi-Stage.

upvoted 2 times

rdemontis 2 years, 5 months ago

Selected Answer: C

IMHO the answer is C
https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/test/publish-test-results?view=azure-devops&tabs=trx%2Cyaml#docker

upvoted 1 times

tatdatpham 2 years, 6 months ago

Selected Answer: C

Multistage is right answer

"Build and test with a multi-stage Dockerfile: build and tests execute inside the container using a multi-stage Docker file, as such test results are not published back to the pipeline."

https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/test/publish-test-results?view=azure-devops&tabs=trx%2Cyaml

upvoted 2 times

Whirly 2 years, 6 months ago

Selected Answer: D

IHOP, Answer is D, because the question mentions "Prevent the results from being published to the pipeline" if you need to publish results then it is multi-stage.

upvoted 1 times

Mev4953 2 years, 6 months ago

Build and test WITHOUT publishing ==> multi-stage

upvoted 1 times

Shreyans 2 years, 7 months ago

Selected Answer: C

Multistage is right answer

upvoted 1 times

Question #43 *Topic 7*

You are designing an Azure DevOps strategy for your company's development team.
You suspect that the team's productivity is low due to accumulate technical debt.
You need to recommend a metric to assess the amount of the team's technical debt.
What should you recommend?

A. the number of code modules in an application

B. the number of unit test failures

C. the percentage of unit test failures

D. the percentage of overall time spent on rework

Suggested Answer: *D*
Technical Debt is the estimated cost to fix code elements issues.
Technical Debt Ratio: Ratio between the cost to develop the software and the cost to fix it. The Technical Debt Ratio formula is:
Remediation cost / Development cost
Which can be restated as:
Remediation cost / (Cost to develop 1 line of code * Number of lines of code)
Reference:
http://www.azure365.co.in/devops/3PDevOps-4

Community vote distribution
D (100%)

roydeen Highly Voted 3 years, 9 months ago
absolutely correct, technical debt is when you do something 'quickly', 'just for now', 'it will be coded later' fashion. hence, rework is often needed
upvoted 25 times

amsun10 2 years, 11 months ago
great explaination
upvoted 5 times

Cluster007 Highly Voted 3 years, 10 months ago
Correct
upvoted 17 times

mrg998 Most Recent 1 year, 8 months ago
Selected Answer: D
yep d for sure
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: D
If the application code has technical debt, this means that the development team is spending time on existing issues. The technical debt would make it difficult to deliver changes faster.

Answer is D
upvoted 1 times

kennynelcon 2 years, 1 month ago
Selected Answer: D
Accurate option
upvoted 1 times

Eltooth 2 years, 4 months ago
Selected Answer: D
D is correct answer.
upvoted 1 times

pandrer 2 years, 4 months ago

Correct answer D

https://devblogs.microsoft.com/premier-developer/technical-debt-the-anti-devops-culture/

upvoted 2 times

rdemontis 2 years, 5 months ago

Selected Answer: D

correct

upvoted 1 times

Question #44 *Topic 7*

You are developing an open source solution that uses a GitHub repository.
You create a new public project in Azure DevOps.
You plan to use Azure Pipelines for continuous build. The solution will use the GitHub Checks API.
Which authentication type should you use?

A. OpenID

B. GitHub App

C. a personal access token (PAT)

D. SAML

Suggested Answer: *B*
Write permission for the Checks API is only available to GitHub Apps.
Note: Authenticating as a GitHub App lets you do a couple of things:
➪ You can retrieve high-level management information about your GitHub App.
➪ You can request access tokens for an installation of the app.
Reference:
https://docs.github.com/en/rest/guides/getting-started-with-the-checks-api

Community vote distribution
B (100%)

mak1 Highly Voted 3 years, 4 months ago
B is Correct.
upvoted 12 times

Kalaismile06 Highly Voted 3 years, 3 months ago
This is repeated question. Given answer is correct.
upvoted 5 times

rumenta Most Recent 10 months, 2 weeks ago
There are three authentication types for granting Azure Pipelines access to your GitHub repositories while creating a pipeline but only GitHub App works with GitHub Checks. B is correct.
https://learn.microsoft.com/en-us/azure/devops/pipelines/repos/github?view=azure-devops&tabs=yaml#access-to-github-repositories
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: B
https://docs.github.com/en/rest/guides/getting-started-with-the-checks-api
https://docs.github.com/en/developers/apps/building-github-apps/authenticating-with-github-apps

Answer is B
upvoted 2 times

Eltooth 2 years, 4 months ago
Selected Answer: B
B is correct answer.
upvoted 1 times

UnknowMan 2 years, 4 months ago
Selected Answer: B
Correct
upvoted 1 times

Cheehp 2 years, 5 months ago
Selected during exam.
B. GitHub App
upvoted 2 times

rdemontis 2 years, 5 months ago

Selected Answer: B

correct

upvoted 1 times

Mev4953 2 years, 6 months ago

GitHub Checks works only with GitHub App

https://docs.microsoft.com/en-us/azure/devops/pipelines/repos/github?view=azure-devops&tabs=yaml#:~:text=There%20are%20three%20authentication%20types%20for%20granting%20Azure%20Pipelines%20access%20to%20your%20Git

upvoted 4 times

Optimist_Indian 2 years, 7 months ago

Got this question in Feb-2022 exam (scored 910+). Given answer is correct.

upvoted 3 times

subrata83 2 years, 11 months ago

Got this in the Az-400 exam(Sep 27 2021)

upvoted 4 times

Question #45 *Topic 7*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has a project in Azure DevOps for a new web application.
You need to ensure that when code is checked in, a build runs automatically.
Solution: From the Continuous deployment trigger settings of the release pipeline, you enable the Pull request trigger setting.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
In Visual Designer you enable continuous integration (CI) by:
1. Select the Triggers tab.
2. Enable Continuous integration.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/get-started-designer

Community vote distribution
B (100%)

DevOpsGeek Highly Voted 3 years, 10 months ago
The answer is correct, but the explanation is wrong, when a new code is checkin, the build will trigger only when we configure the Build Validation in Branch policy for the Main branch
upvoted 17 times

fihdsaHFHVKJFEV324 3 years, 6 months ago
right!
upvoted 1 times

UrbanRellik Most Recent 3 months, 1 week ago
Selected Answer: B
There's multiple parts for this to be a true (A) "yes", statement.

1. Enable a minimum of three reviewers.
2. Authors can review their own code.
3. All merges to main must be submitted in the form of a pull request.

The above criteria has not been confirmed. Therefore, the answer is (B) No.
upvoted 1 times

syu31svc 2 years, 1 month ago
Selected Answer: B
https://docs.microsoft.com/en-us/devops/develop/what-is-continuous-integration

"Continuous integration (CI) is the process of automatically building and testing code every time a team member commits code changes to version control."

Answer is No
upvoted 1 times

rdemontis 2 years, 5 months ago
Selected Answer: B
correct answer but wrong explanation

upvoted 1 times

rdemontis 2 years, 5 months ago
Sorry, the explanation is correct. It refers to the creation of the build pipeline by the classic editor
upvoted 1 times

lugospod 2 years, 7 months ago
Got this January 2022.
upvoted 3 times

ChauPhan 2 years, 10 months ago
I checked the release pipeline on LAB, it displays

Continuous deployment trigger
Git: _python-sample-vscode-flask-tutorial
Enabling the trigger will create a new release every time a Git push happens to the selected repository.
Pull request trigger
Git: _python-sample-vscode-flask-tutorial

Enabling this will create a release every time a selected artifact is available as part of a pull request workflow
upvoted 2 times

ChauPhan 2 years, 10 months ago
So the correct answer is : Continuous deployment trigger is set to ENABLE
upvoted 1 times

ChauPhan 2 years, 10 months ago
The answer for the question is for general pipeline, not release pipeline
upvoted 1 times

MrMonkfish 3 years ago
The requirement is that "You need to ensure that when code is checked in, a build runs automatically.", when code is checked in to perform a build, so Continuous Integration.

The answer "Solution: From the Continuous deployment trigger settings of the release pipeline, you enable the Pull request trigger setting." is talking about Continuous Deployment, which is for deploying, not building.

I say B - No, it is not the correct solution. Enable Continuous Integration instead.
upvoted 3 times

moota 3 years, 2 months ago
My opinion is a PR is different from a code check in.
upvoted 2 times

prashantjoge 2 years, 5 months ago
PR is obviously different from a code checkin
upvoted 1 times

johnny19873 4 years ago
Definitely it's B
upvoted 4 times

Fred64 4 years, 4 months ago
Pull Request trigger is a build pipeline trigger, not release's
upvoted 4 times

zalyoung 4 years, 2 months ago
release pipeline has PR trigger as well

https://docs.microsoft.com/en-us/azure/devops/pipelines/release/triggers?view=azure-devops#prsettrigger
upvoted 2 times

Question #46 *Topic 7*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has a project in Azure DevOps for a new web application.
You need to ensure that when code is checked in, a build runs automatically.
Solution: From the Pre-deployment conditions settings of the release pipeline, you select After stage.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Instead, In Visual Designer you enable continuous integration (CI) by:
1. Select the Triggers tab.
2. Enable Continuous integration.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/get-started-designer

Community vote distribution
B (100%)

27close Highly Voted 3 years, 10 months ago
no- this should be selected before a gate
upvoted 6 times

syu31svc Most Recent 2 years, 1 month ago
Selected Answer: B
https://docs.microsoft.com/en-us/devops/develop/what-is-continuous-integration

"Continuous integration (CI) is the process of automatically building and testing code every time a team member commits code changes to version control."

Answer is No
upvoted 1 times

rdemontis 2 years, 5 months ago
Selected Answer: B
correct answer but wrong explanation
upvoted 1 times

rdemontis 2 years, 5 months ago
Sorry, the explanation is correct. It refers to the creation of the build pipeline by the classic editor
upvoted 1 times